Deelbesluit 1 - Datalekken
Document 1

de Rechtspraak

Draaiboek incidentafhandeling bij datalekken IVO Rechtspraak

datum	6 april 2020
versie	0.7
auteur	mr. [redacted]

Versiebeheer

Versie	Wat	Door wie	Datum
0.1	Initiële opstelling	[redacted]	21-01-2020
0.2	Feedback [redacted] verwerkt	[redacted]	22-01-2020
0.3	Toevoeging stroomschema, verwerking feedback [redacted]	[redacted]	14-02-2020
0.4	Feedback [redacted] verwerkt	[redacted]	07-03-2020
0.5	Aanpassingen stroomschema, tekstuele aanpassingen	[redacted]	19-03-2020
0.6	Review [redacted]	[redacted]	06-04-2020
0.7	Feedback verwerken + laatste tekstuele wijzigingen	[redacted]	06-04-2020
0.8	Feedback verwerken [redacted]	[redacted]	09-06-2020
0.9	Tekstuele wijzigingen	[redacted]	12-09-2020

Inhoudsopgave

1 Inleiding

Inbreuken op persoonsgegevens kunnen worden veroorzaakt door menselijke fouten of door onrechtmatig handelen, bijvoorbeeld door het omzeilen van technische beveiligingsmaatregelen die zijn geïmplementeerd om persoonsgegevens te beschermen of als persoonsgegevens per abuis verstuurd worden naar een verkeerde partij. Het is daarom belangrijk dat IVO Rechtspraak een duidelijke procedure kan volgen waarmee op een verantwoorde wijze gehandeld kan worden om persoonsgegevens te beschermen ten tijde van een inbreuk, en kan handelen binnen de wettelijke termijn die voor afhandeling van een inbreuk gesteld is. Wanneer sprake is van een inbreuk dient IVO Rechtspraak zich enerzijds te focussen op het beschermen van betrokkenen en hun persoonsgegevens en anderzijds op de bescherming van de belangen van IVO Rechtspraak. Dit draaiboek geeft nadere invulling aan het privacybeleid dat door IVO Rechtspraak is vastgesteld en het Handboek Datalekken Gerechten.

2 Definities

Autoriteit Persoonsgegevens	De Nederlandse toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens[1], niet zijnde persoonsgegevens die verwerkt worden in het kader van rechtszaken en de uitoefening van gerechtelijke taken (afgekort: de AP).
AVG	De Algemene verordening gegevensbescherming.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft.
CISO	De Chief Information Security Officer.
Inbreuk in verband met Persoonsgegevens	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens,[2] ook wel datalek genoemd. Een inbreuk op de beveiliging heeft niet automatisch een inbreuk in verband met persoonsgegevens tot gevolg. De inbreuk moet derhalve gevolgen hebben voor persoonsgegevens om te kunnen spreken van een datalek onder de AVG.
Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”): als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden

[1] Art. 4 sub 22 Algemene verordening gegevensbescherming.
[2] Art. 4 sub 12 Algemene verordening gegevensbescherming.

	geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.[3] Met geïdentificeerd of identificeerbaar natuurlijk persoon wordt het onderscheid bedoelt tussen direct en indirect herleidbare persoonsgegevens.
Procureur-Generaal HR	De toezichthoudende autoriteit bij de Hoge Raad die betrokken is bij de verwerking van persoonsgegevens die verwerkt worden in het kader van rechtszaken en de uitoefening van gerechtelijke taken. Dit betreft alle verwerkingen van persoonsgegevens die plaatsvinden in het kader van rechtszaken.
(Verwerkings)verantwoordelijke	Degene die alleen of samen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

3 Doel

Het doel van deze procedure is om de reactie van IVO Rechtspraak op een inbreuk op persoonsgegevens te standaardiseren en ervoor te zorgen dat de afhandeling van de inbreuk geregistreerd en beheerd wordt in overeenstemming met de Algemene verordening gegevensbescherming (AVG). Hiermee kan ervoor worden gezorgd dat daar waar gegevens verkeerd geadresseerd, verloren, gehackt of gestolen worden, of onjuist toegankelijk zijn of beschadigd, het incident op een correcte wijze wordt onderzocht en, indien wettelijk vereist, binnen de juiste termijnen gerapporteerd wordt aan de Autoriteit Persoonsgegevens (AP) of Procureur-Generaal (P-G HR) en in sommige gevallen bovendien tevens direct aan de betrokkenen.

4 Scope

Dit draaiboek is van toepassing op de afhandeling van inbreuken in verband met persoonsgegevens binnen IVO Rechtspraak in de gevallen waar IVO Rechtspraak als verwerkingsverantwoordelijke is aan te merken, en doorgeleiding daarvan aan verwerkersverantwoordelijken zoals de raad en gerechten indien IVO Rechtspraak niet als verantwoordelijke kan worden aangemerkt. De wijze van afhandeling van datalekken waarvoor IVO Rechtspraak geen verwerkersverantwoordelijke is valt buiten de scope van dit beleid. Dit draaiboek dient daarnaast als uitwerking van het Handboek Datalekken Gerechten en de toepassing daarvan binnen IVO Rechtspraak.

[3] Art. 4 sub 1 Algemene verordening gegevensbescherming.

5 Referentiedocumenten

- VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)[4]
- Uitvoeringswet Algemene verordening gegevensbescherming[5]
- Handboek Meldplicht datalekken voor gerechten[6]
- Meldformulier datalekken
- Guidelines meldplicht datalekken[7]
- Wet justitiële en strafvorderlijke gegevens[8]

6 Verantwoordelijkheden

Werknemers IVO Rechtspraak
Alle werknemers van IVO Rechtspraak zijn verantwoordelijk voor het doorgeven van mogelijke inbreuken op persoonsgegevens zodra zij daarvan op de hoogte raken of als er een vermoeden is van een mogelijke inbreuk. Dit wordt gemeld aan team SP&K door middel van het datalekformulier.[9]

Management / proceseigenaar
Het management (bv. projectmanager of teamleider)[10] en/of de proceseigenaar assisteren bij onderzoek naar mogelijke inbreuken op persoonsgegevens. Dit geldt voor inbreuken bij zowel bestaande systemen als bij projecten die systemen bouwen. Daarnaast dragen zij zorg voor het toezien op de implementatie van benodigde beveiligingsmaatregelen om de gevolgen van de inbreuk in te perken.

Functionarissen & Officer Privacy
De Functionarissen Privacy en Officer Privacy bij IVO Rechtspraak zien toe op de afhandeling van de inbreuk op persoonsgegevens op grond van dit Draaiboek, zorgen voor de registratie van het incident in Classbase en stellen de directie van IVO Rechtspraak en de Functionaris Gegevensbescherming van de Raad voor de Rechtspraak na afstemming met de CISO van IVO Rechtspraak op de hoogte van de mogelijke inbreuk.

Functionarissen & Officer Security

[4] Zie https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf.
[5] Zie https://wetten.overheid.nl/BWBR0040940/2018-05-25.
[6] Zie [redacted]
[7] Zie https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf
[8] Zie https://wetten.overheid.nl/BWBR0014194/2020-01-01.
[9] Deze is hier te vinden: [redacted]
[10] Een overzicht van de verantwoordelijke manager per afdeling staat in het organogram op Intro: [redacted]

In veel gevallen zal bij een inbreuk op persoonsgegevens ook sprake zijn van mogelijke beveiligingsrisico's. De functionaris(sen) security en officer security dienen daarom eveneens geïnformeerd te worden over de inbreuk op persoonsgegevens, zodat zij een onderzoek kunnen instellen naar mogelijke beveiligingsrisico's en daaropvolgend advies kunnen uitbrengen over de te implementeren mitigerende maatregelen.

CIO
De CIO besluit in de gevallen waar IVO Rechtspraak aangemerkt kan worden als verwerkingsverantwoordelijke om al dan niet melding te doen van de inbreuk in verband met persoonsgegevens aan de verantwoordelijke toezichthouder en, indien noodzakelijk, aan de betrokkene(n). In de meeste gevallen zal dat zijn in overleg met directeur bureau raad, de BVA of het pro. In geval van gezamenlijke verwerkingsverantwoordelijkheid met de gerechten en/of de Raad voor de Rechtspraak dienen de andere verwerkingsverantwoordelijken geïnformeerd te worden door de CIO.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming wordt door de functionaris / officer privacy op de hoogte gesteld van de mogelijke inbreuk op persoonsgegevens en adviseert de CIO over de inbreuk en of deze gemeld moet worden aan de toezichthouder.

CISO
Bij verstoringen met een hoge impact (calamiteit/crisis) heeft de CISO een coördinerende rol in calamiteiten- en oplosteams. De CISO informeert daarnaast de CIO.

7 Melden van inbreuken in verband met persoonsgegevens (intern)

Indien een medewerker van IVO Rechtspraak op de hoogte raakt van een (mogelijke) inbreuk in verband met persoonsgegevens dient dit direct gemeld te worden aan de aanwezige Functionaris of Officer Privacy, bij voorkeur ook telefonisch en via de mailbox privacy ([redacted]@rechtspraak.nl). Het meldformulier moet volledige en nauwkeurige details van het incident bevatten en de naam van de persoon die het incident rapporteert. Het meldformulier moet worden ingevuld bij het melden van een (vermoedelijke) inbreuk. Daarnaast moet melding gemaakt worden via Topdesk.

8 Reageren op mogelijke inbreuken in verband met persoonsgegevens

Een meldbare inbreuk op persoonsgegevens dient binnen 72 uur (drie kalenderdagen) gemeld te worden aan de verantwoordelijke toezichthouder.[11] Wanneer de inbreuk waarschijnlijk een hoog risico op basis van de afgenomen risicoanalyse[12] inhoudt voor de betrokkenen dient de

[11] Art. 33 lid 1 Algemene verordening gegevensbescherming.
[12] Zie in stap 2 in paragraaf 8.1.2 van dit document de uitleg over de risicoanalyse.

inbreuk ook direct aan hen te worden gemeld.[13] Deze termijn gaat in zodra een inbreuk op persoonsgegevens is vastgesteld door de officer/functionaris Privacy, niet reeds na een vermoeden. Dit hoofdstuk bevat een plan om stapsgewijs tot een gecontroleerde afhandeling van een inbreuk te komen.

De melding van de inbreuk zet het onderstaande incident afhandelingsproces in gang. De volgende stappen dienen in dit proces te worden gevolgd zodra een mogelijk inbreuk is gemeld:

8.1.1 Stap 1: initiële beoordeling en inventarisatie van incident (binnen 24 uur na vaststelling inbreuk)

De functionaris of officer privacy is primair verantwoordelijk voor het beoordelen en onderzoeken van mogelijke en feitelijke inbreuken op persoonsgegevens. De initiële beoordeling en inventarisatie dient het volgende te omvatten:

- Bepalen of daadwerkelijk een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Mogelijk is wel sprake van een inbreuk op de beveiliging, maar waren daar geen persoonsgegevens bij betrokken. In dat geval moet de melding verder afgehandeld worden door de functionaris / officer security.
- Beoordeling of IVO Rechtspraak als (gezamenlijk) verwerkingsverantwoordelijke kan worden aangemerkt voor de gegevens waarop de inbreuk betrekking heeft. Wanneer sprake is van een landelijke dienst, dient de melding te worden afgehandeld door de Raad.
- Wat voor persoonsgegevens betrokken zijn bij de inbreuk.
- Oorzaak van de inbreuk.
- Welke afdeling(en) betrokken is/zijn bij de inbreuk.
- Welke systemen betrokken zijn bij de inbreuk.
- Of sprake is van een mogelijk beveiligingsincident.
- Hoeveel betrokkenen door de inbreuk kunnen worden getroffen.
- Veiligstellen van de betreffende gegevens (zorg ervoor dat deze bijvoorbeeld niet langer voor iedereen toegankelijk zijn, maar verwijder pas zodra de gegevens niet meer nodig zijn voor de verdere afhandeling).

Zodra is vastgesteld dat sprake is van een inbreuk in verband met persoonsgegevens start de termijn van 72 uur waarbinnen mogelijk gemeld moet worden. De afhandeling van het incident moet worden gedocumenteerd. Deze documenten kunnen door de toezichthouder worden beoordeeld en moeten goed worden bijgehouden om traceerbaarheid en verantwoording te garanderen.

Zodra is vastgesteld dat een inbreuk in verband met persoonsgegevens heeft plaatsgevonden dient een incident responsteam samengesteld te worden dat verantwoordelijk wordt voor de verdere afhandeling van de inbreuk op persoonsgegevens. Dit team moet in ieder geval bestaan uit:

- Functionaris / officer privacy
- Functionaris / officer security
- CISO

[13] Art. 34 lid 1 Algemene verordening gegevensbescherming.

- De verantwoordelijke dienstenmanagers en/of service delivery manager

De officer privacy is verantwoordelijk voor het samenstellen van het incident responsteam en fungeert bij de afhandeling als procesbegeleider. Bij afwezigheid van de officer privacy wordt het incident responsteam samengesteld door één van de dienstdoende functionarissen privacy en wordt de functionaris aangewezen als procesbegeleider. De procesbegeleider wijst een van de teamleden aan die verantwoordelijk gemaakt wordt voor het verzamelen en bijhouden van de documentatie voor afhandeling van de inbreuk. Dit zal doorgaans de functionaris of officer privacy zijn. De procesbegeleider betrekt daarnaast een functionaris en/of officer security en indien noodzakelijk de CISO en verantwoordelijke dienstenmanager en/of service delivery manager. Daarnaast kan de FG reeds in dit stadium worden ingelicht en/of om advies worden gevraagd over de verdere afhandeling van het incident. Daarnaast wordt de (gedelegeerde) manager/proceseigenaar ingelicht over de inbreuk. De (gedelegeerde) manager/proceseigenaar is verantwoordelijk voor het inlichten van overige sleutelfiguren rondom de dienst/systeem/het proces waarop de inbreuk betrekking heeft (bv. de portefeuillehouder, product owner, service delivery manager).

8.1.2 Stap 2: risicobeoordeling en berichtgeving aan CIO en FG (binnen 48 uur na vaststelling inbreuk)

De potentiële risico's die voortvloeien uit een inbreuk in verband met persoonsgegevens moeten worden bepaald en er moet rekening worden gehouden met mogelijke negatieve gevolgen voor betrokkenen, bijvoorbeeld hoe waarschijnlijk het is dat de negatieve gevolgen zullen optreden en hoe ernstig en substantieel deze kunnen zijn. De risico’s en impact voor betrokkenen ten gevolge van een inbreuk kunnen verschillen en moeten bij elke inbreuk opnieuw afgewogen worden. Wanneer een inbreuk plaatsvindt is het van belang de verwerkingsverantwoordelijke de inbreuk onder controle krijgt, maar ook direct een inschatting maakt van het risico voor de betrokkene.

Om de ernst van de inbreuk te bepalen moet een initiële risicobeoordeling gedaan worden waarmee een inschatting gedaan kan worden met betrekking tot de ernst van de inbreuk. Deze risicobeoordeling wordt gedaan door de functionaris of officer privacy, waar nodig met ondersteuning van de (gedelegeerde) manager/proceseigenaar om de inbreuk in kaart te brengen op basis van onderstaande vragen.

Bij de risicobeoordeling komen in ieder geval de volgende punten aan bod:

- Hoeveel betrokkenen zijn getroffen?
- Wiens persoonlijke gegevens zijn geschonden? Gaat het om gegevens van kwetsbare betrokkenen (bijvoorbeeld kinderen)?
- Wat is de aard van de persoonsgegevens die bij de inbreuk zijn betrokken? Gaat het om risicovolle persoonsgegevens?
- Vormt de inbreuk een risico voor reputatie, identiteitsdiefstal, veiligheid en / of financieel verlies van getroffen personen?
- Hoe ernstig of substantieel zijn deze gevolgen?
- Hoe waarschijnlijk zijn de risico's?
- Zijn er aanvullende maatregelen geïmplementeerd om de impact van een mogelijke inbreuk te minimaliseren? (Dit kunnen technische maatregelen zijn, zoals

pseudonimisering van persoonsgegevens, die bijvoorbeeld zijn vastgesteld op basis van een afgenomen PIA en risicoanalyse).

Het is afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen of een datalek gemeld moet worden. Wanneer wordt vastgesteld dat de inbreuk waarschijnlijk zal leiden tot een risico voor de rechten en vrijheden van natuurlijke personen, moet de inbreuk worden gemeld aan de betrokken toezichthoudende autoriteit. Wanneer de inbreuk waarschijnlijk een hoog risico inhoudt voor de betrokkenen dient de inbreuk ook direct aan hen te worden gemeld. Wanneer uit de risicoanalyse volgt dat de impact van de inbreuk voor betrokkenen als laag kan worden ingeschat wordt geadviseerd om de inbreuk niet te melden, omdat het in dat geval niet waarschijnlijk wordt geacht dat de inbreuk leidt tot een risico voor de rechten en vrijheden van betrokkenen. Daarnaast moet een initieel advies over de mogelijke voorgenomen beveiligingsmaatregelen gedaan worden door de functionaris of officer security om de risico's te mitigeren.

Zodra de risicobeoordeling afgerond is dient een memo aan CIO opgesteld te worden met de bevindingen. De CIO dient tijdig, en uiterlijk binnen 48 uur na vaststelling van de inbreuk op de hoogte gesteld te worden van het incident. De CIO moet voldoende tijd hebben om een afweging te maken of een datalek gemeld moet worden aan de toezichthouder en/of betrokkene(n) en om zich voor te kunnen bereiden op verschillende scenario's (bijvoorbeeld aandacht van de media). Dit memo wordt opgesteld door de functionaris of officer privacy en wordt verstuurd naar de CIO van IVO Rechtspraak. Het memo dient tevens te worden verstuurd naar de functionaris gegevensbescherming van de Raad voor de Rechtspraak.

Het memo bevat minimaal een beschrijving van het incident, wanneer dat bekend is geworden, wie daarbij betrokken en daarvan op de hoogte zijn en een beschrijving van de voorgenomen maatregelen. Daarnaast bevat het memo de risicobeoordeling betreffende de mogelijke impact (risico's) voor betrokkene(n). Het memo heeft als doel om de CIO te ondersteunen in het maken van een weloverwogen en goed onderbouwde beslissing om al dan niet over te gaan tot melden aan de toezichthouder, dan wel aan de betrokkene(n). De Functionaris Gegevensbescherming kan daarnaast op grond van het memo advies om wel of niet te melden uitbrengen aan de CIO.

8.1.3 Stap 3: melding van de inbreuk (binnen 72 uur na vaststelling inbreuk)

Zodra is besloten[14] om tot dat worden gedaan door het volgende formulier op de website van de Autoriteit Persoonsgegevens in te vullen:
https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1.
De melding aan de P-G HR kan gedaan worden middels het volgende meldformulier:
https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Hoge-Raad-der-Nederlanden/Documents/Formulier%20melding%20datalek.pdf.
Als het waarschijnlijk is dat de inbreuk hoge risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt, moet de inbreuk ook zo spoedig mogelijk en zonder onnodige vertraging door de verwerkingsverantwoordelijke aan de betrokkene worden meegedeeld. Dit moet rechtstreeks aan de betrokkene worden meegedeeld, tenzij dit onevenredige inspanningen zou vergen.

[14] In hst. 3 van het Handboek Datalekken Gerechten is nader uitgewerkt wanneer een datalek gemeld dient te worden.

Als dit laatste het geval is, kan de inbreuk ook worden gecommuniceerd via openbare kanalen zoals sociale media of een bericht in een krant. De meest effectieve manier moet worden gekozen. De communicatie naar de betrokkenen moet een duidelijk en specifiek advies omvatten met betrekking tot maatregelen die zij kunnen nemen om zichzelf te beschermen tegen de gevolgen van de inbreuk, en in hoeverre IVO Rechtspraak hen daarbij kan bijstaan. Het bericht dient daarnaast contactgegevens te bevatten waarop betrokkenen contact kunnen opnemen met de organisatie.[15]
Bij externe communicatie dient rekening gehouden te worden met de gevolgen en impact voor de organisatie. Inbreuken kunnen media-aandacht genereren waar adequaat op gereageerd moet worden. Betrek in dat geval de afdeling Communicatie.[16] Verkeerde communicatie kan schadelijk zijn voor het imago van de organisatie, maar kan ook onnodig extra paniek veroorzaken bij de betrokkene(n).

Als de inbreuk is veroorzaakt door een strafrechtelijk feit kan daarnaast aangifte gedaan worden in overleg met de CIO.

8.1.4 Stap 4: inperking van de inbreuk en mitigerende maatregelen

Wanneer een inbreuk heeft plaatsgevonden, moet actie ondernomen worden om de gevolgen van de inbreuk te beperken. Deze stap kan gelijktijdig met de voorgaande stappen doorlopen worden. Bij onderzoek naar mogelijke beveiligingsrisico's dient een functionaris of officer security betrokken te worden, waarna zij een advies uit moeten brengen over de te nemen mitigerende maatregelen om de gevolgen van de inbreuk te beperken. Indien onderzoek gedaan moet worden in systemen met daarin gevoelige persoonsgegevens wordt daarvoor toestemming gevraagd bij de directie conform het securitybeleid. De volgende maatregelen kunnen worden overwogen:

- Sluit een gecompromitteerd systeem af dat tot de inbreuk heeft geleid.
- Bepaal of en welke stappen kunnen worden genomen om verloren gegevens te herstellen en eventuele schade als gevolg van de inbreuk te beperken.
- Verhinder verdere ongeautoriseerde toegang tot het systeem.
- Stel wachtwoorden opnieuw in als accounts en / of wachtwoorden zijn gecompromitteerd.
- Isoleer de oorzaken van de inbreuk in het systeem en wijzig indien van toepassing de toegangsrechten tot het gecompromitteerde systeem en verwijder externe verbindingen.
- Ga na of er iets kan worden gedaan om verloren gegevens te herstellen (bijvoorbeeld door back-uptapes te gebruiken)

Bepaal vervolgens wie betrokken moet worden bij de implementatie van de maatregelen. Hierbij kan worden gedacht aan de dienstenmanagers van de verschillende afdelingen bij IVO Rechtspraak. De verwerkingsverantwoordelijke is verantwoordelijk voor het nemen van mitigerende maatregelen nadat advies is uitgebracht door de functionaris/officer privacy en/of de functionaris/officer security.

---

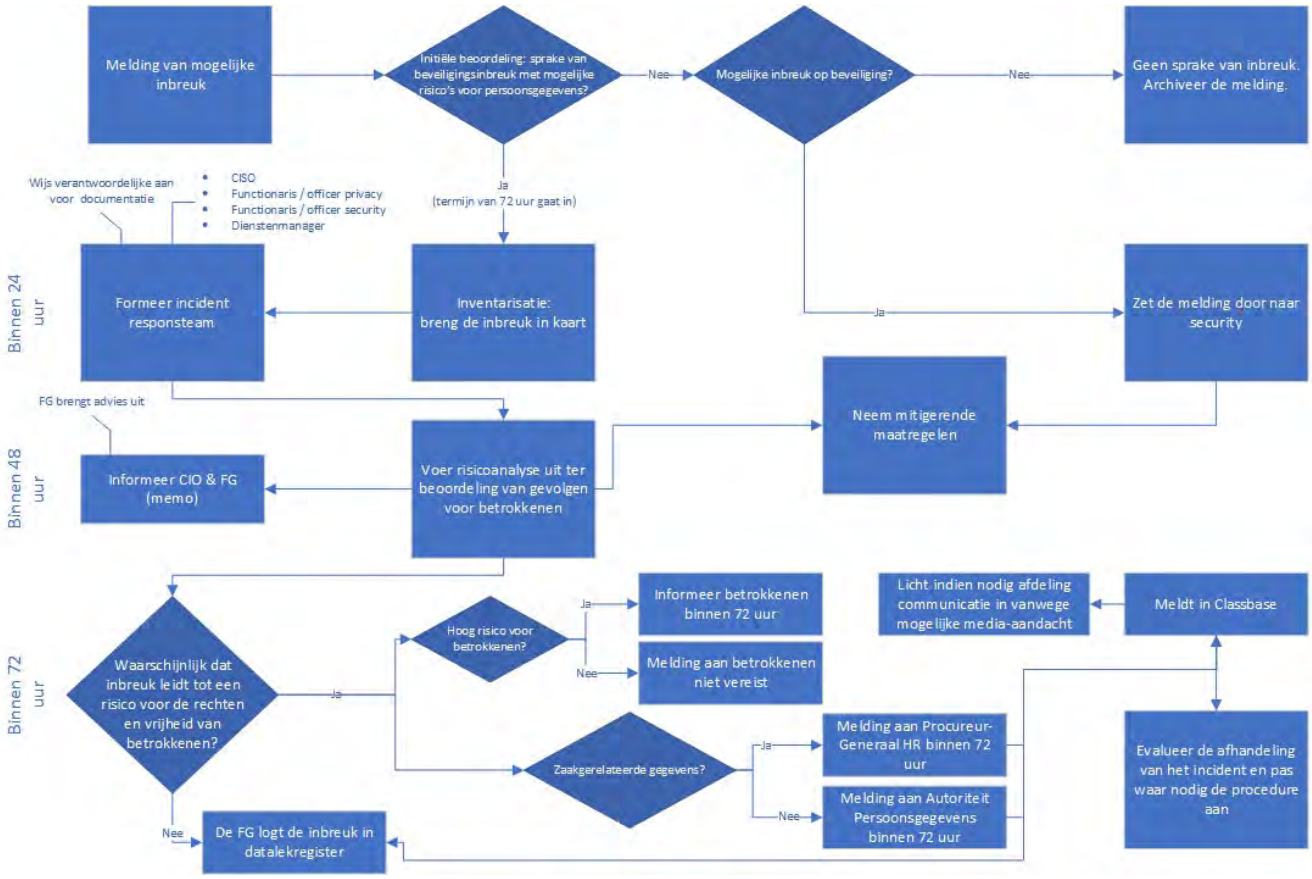
[15] De w jze waarop deze melding moet worden gedaan is nader uitgewerkt in hst. 3.5 van het Handboek Datalekken Gerechten.
[16] Zie [redacted]

8.1.5 Stap 5: evaluatie en lessons learned

Na afronding van bovenstaande procedures en afhandeling van de inbreuk moet het proces in draaiboek worden geëvalueerd en waar nodig aangepast worden in gezamenlijk overleg met degene die betrokken waren bij de afhandeling van de inbreuk. Dit heeft als doel om te controleren of de tijdens het incident genomen stappen passend waren en om te bepalen of en op welke punten de procedure moet worden verbeterd.

Daarnaast moet worden overwogen of verdere actie nodig is om het risico op toekomstige inbreuken te verminderen en de impact van een dergelijke inbreuk te minimaliseren. Reeds geïmplementeerde technische beveiligingsmaatregelen moeten worden geëvalueerd en moeten mogelijk worden bijgewerkt. Ook moet worden overwogen of personeel en gebruikers van het systeem voldoende zijn opgeleid in het gebruik daarvan. Mogelijk is het noodzakelijk dat werknemers of gebruikers een privacy awareness training volgen.

9 Beslisboom



Deelbesluit 1 - Datalekken
Document 2

Strategisch plan
Privacy

Inhoud

1 Resumé

1.1 Aanleiding

Op 25 mei 2018 wordt het nieuwe Europese privacykader, waaronder de Algemene verordening gegevensbescherming ('AVG') en de Richtlijn gegevensbescherming opsporing en vervolging ('de Richtlijn'), van toepassing en vervalt de huidige Wet bescherming persoonsgegevens ('Wbp'). Zowel de AVG als de Richtlijn zijn van toepassing op de Rechtspraak. De Richtlijn voor de verwerking van persoonsgegevens in strafzaken en de AVG voor de overige gegevensverwerkingen.

1.2 Doel

Om op korte termijn te voldoen aan de nieuwe privacywet- en regelgeving en om een hoger niveau van privacybescherming te bereiken, is besloten om binnen de Rechtspraak een strategie op het gebied van privacy te formuleren. Om deze strategie te bepalen, heeft er op verzoek van Kees Sterk (portefeuillehouder privacy) op 26 april 2017 een strategiesessie op bestuurlijk niveau plaatsgevonden waarin gerechten, landelijke diensten en de Raad voor de rechtspraak ('Raad') vertegenwoordigd waren. Het plan bevat uitsluitend de zienswijze van de Rechtspraak ten aanzien van de wijze waarop uitvoering gegeven dient te worden aan de aankomende privacywetgeving. Het plan bevat dus geen concrete beleidsinvulling van alle belangen die spelen binnen de Rechtspraak en de wijze waarop privacy zich tot deze belangen verhoudt.

1.3 Belangrijkste conclusies

Visie (p. 6 – 11)

- Het algemene uitgangspunt is dat er te allen tijde in overeenstemming met de privacywetgeving wordt gehandeld. Dit waarborgt een zorgvuldige gegevensverwerking. Het is wel van belang dat er naast het belang van privacy ook rekening wordt gehouden met andere belangen, zoals de openbaarheid van de Rechtspraak. Waar de privacywetgeving middels open normen enige ruimte laat voor argumentatie, zal de Rechtspraak daar met eigen beleid invulling aan geven. De Rechtspraak heeft er daarbij voor gekozen om bij de invulling van de open normen rekening te houden met de hoedanigheid waarin de Rechtspraak handelt. Wanneer de Rechtspraak handelt in zijn hoedanigheid als rechtsprekende macht en gegevens verwerkt ten behoeve van het primaire proces, alsmede gegevens die gerelateerd zijn aan het primair proces zullen de open normen in de privacywetgeving strikt geïnterpreteerd worden en zal een hoog ambitieniveau worden nagestreefd.[1] Daarbij is het uitgangspunt: hoe gevoeliger de gegevens, hoe hoger het ambitieniveau. Waar de Rechtspraak opereert als zijnde ieder andere organisatie zullen de open normen – waar mogelijk – minder strikt geïnterpreteerd worden. Ook hierbij geldt: hoe gevoeliger de gegevens, hoe hoger het ambitieniveau. Opgemerkt dient te worden dat er vanzelfsprekend binnen de grenzen van de wet wordt gehandeld. (p. 6 – 9)

- Naast het feit dat de Rechtspraak veel waarde hecht om op een zorgvuldige wijze om te gaan met persoonsgegevens, heeft de Rechtspraak als staatsmacht ook een belangrijke functie om openbaarheid te betrachten richting de maatschappij. Daarbij dient in sommige gevallen een afweging te worden gemaakt tussen deze verschillende belangen. Het is in dergelijke gevallen altijd belangrijk om – in samenspraak met de medewerkers die belast zijn met privacy binnen de Rechtspraak – een gedegen belangenafweging te maken. (p. 10)

- Binnen de Rechtspraak is er aandacht voor innovatie, zoals de ontwikkelingen op het gebied van big data en open data. Bij het uitvoeren van dergelijke experimenten spelen de

[1] Het ambitieniveau is het beoogde niveau wat bij de naleving van de privacywetgeving zal worden nagestreefd. Hoe hoger het ambitieniveau, hoe strikter de open normen geïnterpreteerd zullen worden en hoe zorgvuldiger met de persoonsgegevens zal worden omgegaan.

privacyaspecten een belangrijke rol. Het is derhalve van belang dat bij de opstart, ontwikkeling en uitrol van dergelijke experimenten altijd één van de medewerkers die belast is met privacy binnen de Rechtspraak wordt betrokken. Er zal goed gekeken dienen te worden naar welke gegevens daarbij wel en welke niet verstrekt kunnen worden. Waar mogelijk zal gebruik worden gemaakt van geanonimiseerde gegevens. Bij het uitvoeren van dergelijke experimenten dient er in elk geval altijd in overeenstemming met de privacywetgeving te worden gehandeld. (p. 10)

- Een belangrijk aandachtspunt is dat binnen de Rechtspraak – gelet op de aard van de organisatie – al veel aandacht is voor een zorgvuldige omgang met zaakgegevens van betrokkenen. Bij de implementatie van de aankomende privacywetgeving zal hier zoveel mogelijk op worden voortgeborduurd. Het is van belang dat de privacywetgeving zo gestructureerd mogelijk wordt ingebed in de organisatie, zodat voorkomen wordt dat rechters en medewerkers van de Rechtspraak geconfronteerd worden met een grote hoeveelheid nieuwe regelgeving en procedurele veranderingen en zij zo min mogelijk belemmerd worden in de uitvoering van hun werkzaamheden. (p. 11)

- Een ander belangrijk aandachtspunt is dat er niet alleen nieuw beleid dient te worden ontwikkeld, maar dat de aankomende privacywetgeving ook in huidige processen en procedures doorgevoerd dient te worden. Er dient bij de ontwikkeling van beleid op landelijk niveau derhalve ook aandacht te zijn voor de aanpassing van huidig beleid. Hierbij wordt opgemerkt dat het huidige beleid niet alleen ziet op gedigitaliseerde systemen, maar ook nog op fysieke dossiers. (p. 11)

Beleggen rollen en verantwoordelijkheden (p. 12 – 19)

- Om de aankomende privacywetgeving zo gestructureerd mogelijk in te bedden in de organisatie, is besloten om bij het beleggen van de rollen en verantwoordelijkheden aan te sluiten bij bestaande structuren. Meer specifiek bij de wijze waarop beveiliging binnen de Rechtspraak op dit moment is ingeregeld. Nu nog veel nieuw beleid dient te worden ontwikkeld en getracht wordt de gerechten zo min mogelijk te belasten met de ontwikkeling hiervan, is ervoor gekozen de verantwoordelijkheid voor het privacy beleid zoveel mogelijk landelijk te beleggen. Het gaat hierbij zowel om de ontwikkeling van het beleid als het toezicht daarop. De normenkaders en richtlijnen zullen landelijk ontwikkeld worden en voorts dienen te worden uitgerold bij gerechten en landelijke diensten. De Functionaris Gegevensbescherming ('FG') zal zowel omtrent de advisering over de wetgeving als het toezicht op de naleving een belangrijke rol spelen. Dit betekent dat de huidige rol van de FG uitgebreid dient te worden. Voor de inrichting van de rol van FG zal aansluiting gezocht worden bij de manier waarop de huidige rol van de landelijk beveiligingsambtenaar is ingericht. (p. 12 – 14)

- De FG krijgt, in overeenstemming met de aankomende wetgeving, een belangrijke functie bij het toezien op de naleving van de aankomende privacywetgeving in de gehele organisatie. De FG zal de gerechten en landelijke diensten van advies voorzien, maar daarnaast ook de bevoegdheid hebben om gerechten en landelijke diensten erop te wijzen als zij niet voldoen aan de privacywetgeving. De gerechten en/of de Raad blijven echter wel zelf te allen tijde de verwerkingsverantwoordelijke.[2] De verantwoordelijkheid voor de naleving van de wetgeving kan niet bij de FG komen te liggen. De verwerkingsverantwoordelijke, te weten de Raad en/of gerechten, zijn degene die er uiteindelijk op toe dienen te zien en moeten kunnen aantonen dat zij voldoen aan de vereisten uit de AVG en de Richtlijn. (p. 15 – 17)

- Om op adequate wijze uitvoering te geven aan de privacywetgeving, wordt het tevens nodig geacht een privacy officer aan te stellen bij de landelijke diensten, Spir-it en LDCR. Gelet op het feit dat het zwaartepunt van het aantal privacyvraagstukken bij Spir-it ligt, wordt het aangeraden de privacy officer te positioneren bij Spir-it en onder verantwoordelijkheid van Spir-it te laten vallen. De privacy officer zal naar alle waarschijnlijkheid het merendeel van zijn werkzaamheden voor Spir-it verrichten, maar

[2] De verwerkingsverantwoordel jke is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; zie H5 beleggen rollen en verantwoordelijkheden (p. 13) voor meer uitleg over de verwerkingsverantwoordelijke binnen de Rechtspraak.

dient tevens privacyvraagstukken van het LDCR te ondervangen. Op bestuurlijk niveau dient besloten te worden op welke wijze de verdeling van de werkzaamheden tussen Spir-it en LDCR concreet vormgegeven zal worden. Door aanstelling van een privacy officer wordt in een vroeg stadium aan de 'voorkant' van het proces al veel aandacht besteedt aan de vereisten die voortvloeien uit de privacywetgeving en worden al veel privacyvraagstukken ondervangen. Waar mogelijk zullen meteen aanpassingen worden doorgevoerd om overeenstemming met de privacywetgeving te bereiken. Van belang is dat de functie van de privacy officer los gezien dient te worden van de rol van de FG. De FG zal de taken vervullen zoals deze zijn neergelegd in de AVG en de Richtlijn en dient toe te zien op de naleving van de wetgeving binnen de organisatie. De FG kan daarnaast – middels normenkaders en richtlijnen – adviseren en informeren omtrent de wettelijke vereisten die voortvloeien uit de AVG en de Richtlijn. De privacy officer zal verantwoordelijk zijn voor de operationalisering binnen Spir-it en zal de landelijk opgestelde normenkaders en beleid vertalen naar concrete maatregelen. De privacy officer ondervangt daarnaast het merendeel van de privacyvraagstukken waar medewerkers van Spir-it en – waar nodig – LDCR in hun werkzaamheden tegen aan lopen. (p. 17 – 18)

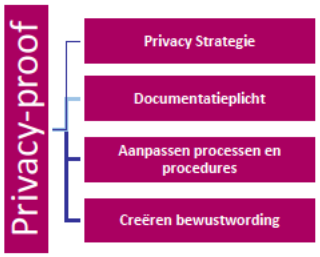
- Om de gerechten zo min mogelijk te belasten met de implementatie van de aankomende privacywetgeving, zullen de verantwoordelijkheden binnen de gerechten niet worden herbelegd. Ook binnen de landelijke dienst SSR zullen de verantwoordelijkheid niet worden herbelegd. De wijze waarop privacy thans is ingericht bij de gerechten en het SSR zal dan ook worden voortgezet. Dat betekent dat de gerechten en het SSR een aanspreekpunt privacy hebben waarmee de FG contact kan opnemen omtrent kwesties rondom privacy. (p. 13 - 14)

- De inbedding van de aankomende privacywetgeving wordt landelijk geregeld. Om het beleid voorts uit te kunnen rollen en in te kunnen bedden bij gerechten en landelijke diensten, is het van belang dat binnen de gerechten en landelijke diensten – op bestuurlijk niveau – draagvlak is voor privacy en bewustwording wordt gecreëerd onder de medewerkers. (p. 16 - 17)

1.4 Actiepunten

Tijdens de strategiesessie zijn er keuzes gemaakt omtrent de visie op het gebied van privacy en beslissingen genomen omtrent het beleggen van de verantwoordelijkheden op het gebied van privacy.
Op basis van onderhavig plan, dienen de medewerkers die belast zijn met privacy binnen de Rechtspraak spoedig te starten met het vormgeven van de vervolgstappen. De vervolgstappen zijn in bijlage I op schematische wijze gevoegd bij dit strategische plan. (p. 20 – 23)

2 Inleiding



Op 25 mei 2018 wordt het nieuwe Europese privacykader, waaronder de AVG en de Richtlijn, van toepassing en vervalt de huidige Wbp. Zowel de AVG als de Richtlijn zijn van toepassing op de Rechtspraak. De Richtlijn voor de verwerking van persoonsgegevens in strafzaken en de AVG voor de overige gegevensverwerkingen. Ten opzichte van de huidige wet introduceren de AVG en de Richtlijn een aanzienlijk aantal nieuwe wettelijke vereisten, waaronder de documentatieplicht, de verplichting van privacy by design[3] en het voeren van een actief gegevensbeschermingsbeleid. Om privacy op professionele wijze in te bedden binnen de Rechtspraak en om in overeenstemming met de wetgeving te handelen, dienen er op korte termijn aanpassingen en verbeteringen te worden doorgevoerd. Indien er niet wordt voldaan aan de wettelijke vereisten, kan de Autoriteit Persoonsgegevens ('AP') onder de AVG boetes opleggen die kunnen oplopen tot 20 miljoen euro.[4] Daarnaast kan een overtreding ook grote gevolgen met zich meebrengen voor de reputatie van en het vertrouwen in de Rechtspraak. Op grond van de AVG en Richtlijn hebben betrokkenen het recht om onder bepaalde voorwaarden een voorziening in rechte in te stellen indien de betrokkene van mening is dat de verwerking van persoonsgegevens inbreuk maakt op de bij de AVG en Richtlijn vastgestelde bepalingen.[5] De Rechtspraak is dan ook 'toezichthouder' op de wet en mede daarom is het belangrijk dat de Rechtspraak als organisatie ook zelf op juiste wijze uitvoering geeft aan de privacywetgeving.

Binnen de Rechtspraak wordt het belang van privacy en de noodzaak van een juiste borging van privacy al enigszins erkend. Een heldere visie hoe privacy binnen de Rechtspraak op gestructureerde wijze kan worden ingebed ontbreekt echter nog. Op dit moment gebeurt er nog te veel op ad hoc en incidentele basis. Om een hoger niveau te bereiken en om op korte termijn te voldoen aan de nieuwe privacywet- en regelgeving, is het noodzakelijk om spoedig te starten met het doorvoeren van acties en verbeteringen. Om op gestructureerde wijze invulling te kunnen geven aan privacy, is het van belang om binnen de Rechtspraak een privacy beleid in te richten. Het startpunt van de inrichting van het privacy beleid is het formuleren van een privacy strategie.

Om deze strategie op het gebied van privacy te bepalen, heeft er op 26 april 2017 een strategiesessie plaatsgevonden. Tijdens deze bijeenkomst waren aanwezig Kees Sterk (lid Raad, alsmede portefeuillehouder privacy), Frans van Dijk (directeur Raad), [redacted] (directeur Spir-it), Linda van der Sloot-van der Zwaard (directeur LDCR), Elmar Jonasse (SBO), [redacted] (Voorzitter GLO), [redacted] (afdelingshoofd Communicatie), [redacted] (Voorzitter Dagelijks bestuur archivarissen), [redacted] (adviseur recht en ICT), [redacted] (adviseur recht en ICT). [redacted] (uitvoerend CIO) was helaas verhinderd deel te nemen aan de sessie. Onderhavig plan bevat de bevindingen uit deze bijeenkomst. Tijdens deze bijeenkomst zijn beslissingen genomen omtrent de algemene visie op het gebied van privacy en de wijze waarop de visie binnen de organisatie zal worden uitgerold. Op basis van onderhavig plan dienen de medewerkers die belast zijn met privacy binnen de Rechtspraak de visie te vertalen naar de door de privacywetgeving gestelde normen en de vervolgstappen vorm te geven. Het plan bevat uitsluitend de zienswijze van de Rechtspraak ten aanzien van de wijze waarop uitvoering gegeven dient te worden aan de aankomende privacywetgeving. Het plan bevat dus geen concrete beleidsinvulling van alle belangen die spelen binnen de Rechtspraak en de wijze waarop privacy zich tot deze belangen verhoudt.

---

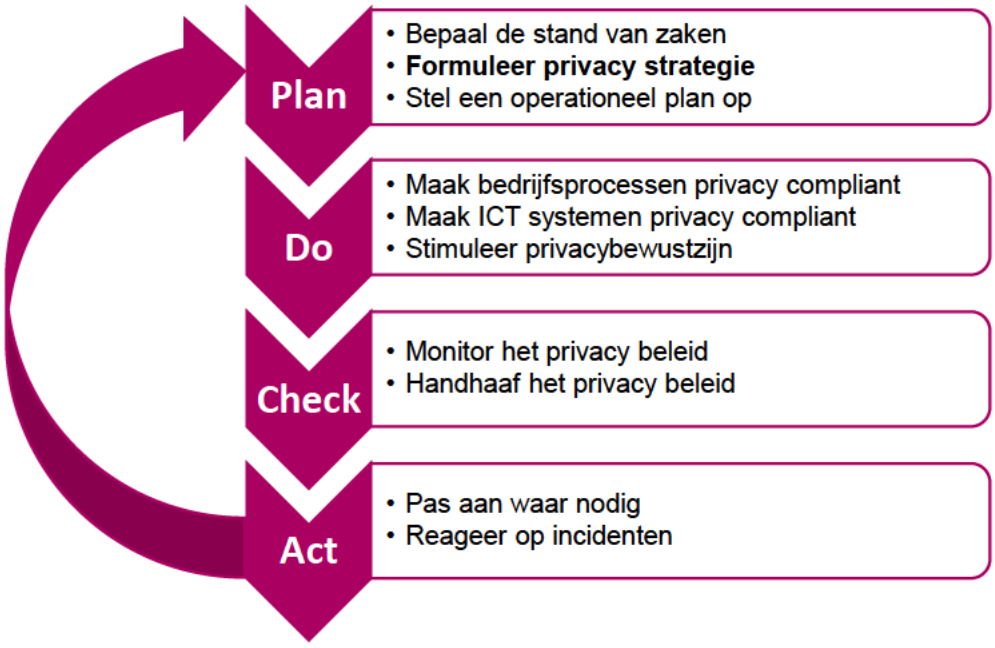
[3] Art kel 25 AVG en art kel 20 Richtlijn. Het beginsel van privacy by design regelt het inbedden van privacy criteria in de ontwerpen en het beheer (van delen) van informatiesystemen, en het inbedden van de privacy maatregelen in de technologie. Dit leidt er toe dat privacy in een vroeg stadium wordt verankerd in de concretisering van informatiebehoefte en het ontwerp.
[4] Art kel 83 lid 5 AVG. In de richtlijn is de vaststelling van straffen aan de lidstaten zelf overgelaten. De lidstaten dienen echter wel de nodige maatregelen te treffen om ervoor te zorgen dat deze straffen worden toegepast. De straffen dienen doeltreffend, evenredig en afschr kkend te zijn. Deze straffen zullen nader worden uitgewerkt in de Wpg en de Wjsg.
[5] Art kel 77 – 79 AVG, artikel 52 – 52 Richtl jn.

3 Privacy beleid: theoretisch kader

3.1 Privacy beleid

Wil de Rechtspraak op een goede en zorgvuldige manier omgaan met de privacy van betrokkenen en de verwerking van persoonsgegevens, dan moet de gehele organisatie daar op ingericht zijn. Dit vereist een bepaalde mate van privacybewustzijn bij de medewerkers en een gestructureerde aanpak. Een goed privacy beleid zorgt ervoor dat een organisatie consequent en gecoördineerd met privacy en de bescherming van persoonsgegevens aan de slag gaat waardoor het risico op non-compliance wordt verminderd. Met een gestructureerd privacy beleid kan de Rechtspraak bovendien jegens de AP aantonen dat het op een verantwoordelijke manier omgaat met persoonsgegevens (accountability). Dit is een belangrijke wettelijke eis uit de AVG en Richtlijn.[6] Het sluitstuk van een goed privacy beleid is monitoring en handhaving. Door het monitoren van het privacy beleid kan het beleid worden bijgestuurd waar nodig. Handhaving zorgt ervoor dat het belang van privacy wordt onderstreept. Vaak draagt handhaving ook bij aan het versterken van privacy-bewustzijn binnen de organisatie en bij het vasthouden van het privacy beleid op lange termijn. Om een goed privacy beleid op te stellen en in te richten, wordt gebruik gemaakt van de Plan-Do-Check-Act cyclus van Deming.

Figuur 1. Plan-Do-Check-Act cyclus



3.2 Startpunt: opstellen privacy strategie

Het startpunt voor de inrichting van een gestructureerd privacy beleid is het vaststellen van de privacy strategie. De AVG en de Richtlijn, bevatten veel open normen en laten enige ruimte voor argumentatie, dit zijn de zogeheten 'grijze gebieden'. Deze ruimte in de wet dwingt de Rechtspraak om met 'eigen' beleid invulling te geven aan de door de privacywetgeving gestelde open normen. Middels deze open normen wordt een verantwoordelijke verplicht goed na te denken omtrent de keuzes die worden gemaakt bij de verwerking van persoonsgegevens. Middels het formuleren van een privacy strategie kan door de Rechtspraak op strategische wijze richting worden gegeven aan die ruimte voor invulling en argumentatie uit de privacywetgeving.

[6] In de AVG is het vereiste van accountability opgenomen in artikel 5 lid 2. In de Richtlijn is het vereiste van accountability vastgelegd in artikel 4 lid 4.

4 Privacy strategie

4.1 Algemene Visie

Het is voor de Rechtspraak van belang om op zorgvuldige wijze met de privacy en persoonlijke gegevens van betrokkenen om te gaan, waarbij het zowel gaat om gegevens van betrokkenen die verwerkt worden ten behoeve van het primaire proces (hieronder vallen tevens gegevensverwerkingen gerelateerd aan het primaire proces) als gegevens van medewerkers van de Rechtspraak. De Rechtspraak hecht er waarde aan om transparant te zijn over het privacy beleid dat zij hanteert en de gegevens die zij verwerkt. Vanzelfsprekend zal er door de Rechtspraak te allen tijde in overeenstemming met de wetgeving worden gehandeld. Dit waarborgt een zorgvuldige gegevensverwerking.

Het is wel van belang dat er naast het belang van privacy ook rekening wordt gehouden met andere belangen, zoals de openbaarheid van de Rechtspraak. Waar de privacywetgeving dan ook enige ruimte laat voor argumentatie, zal de Rechtspraak daar met eigen beleid invulling aan geven. Tijdens de strategiesessie zijn er door de aanwezigen keuzes gemaakt omtrent de invulling van het beleid. Een belangrijke uitkomst hiervan is dat bij de invulling van de open normen rekening gehouden wordt met de hoedanigheid waarin de Rechtspraak handelt. Wanneer de Rechtspraak handelt in de hoedanigheid van rechtsprekende macht en gegevens worden verwerkt ten behoeve van het primaire proces, dienen de open normen in de wetgeving strikt geïnterpreteerd te worden en zal een hoog ambitieniveau worden nagestreefd. Gelet op het feit dat in het primaire proces veelal gegevens worden verwerkt die gevoeliger van aard zullen zijn en het in het merendeel van de gevallen zal gaan om zaken die van groot belang zijn voor betrokkenen, dienen procespartijen er vanuit te kunnen gaan dat er zorgvuldig omgegaan wordt met hun gegevens. Het is belangrijk dat betrokkenen veel vertrouwen hebben in de Rechtspraak en derhalve zal een hoog ambitieniveau worden nagestreefd wanneer het gaat om gegevens die worden verwerkt in het primaire proces.
Wanneer de Rechtspraak handelt als zijnde ieder andere organisatie, waarbij gedacht moet worden aan gegevensverwerkingen die meer van organisatorische aard zijn, zal er – waar mogelijk – meer gebruik worden gemaakt van de open normen die de privacywetgeving biedt.

Nu niet alle gegevens van even gevoelige aard zijn, is het mogelijk om binnen voornoemd beleid de open normen – waar mogelijk – op andere wijze te interpreteren en een hoger of lager ambitieniveau na te streven. Daarbij is besloten dat hoe gevoeliger de gegevens van aard zijn, hoe strikter de normen geïnterpreteerd dienen te worden en hoe hoger het ambitieniveau zal zijn. Deze nuancering maakt het mogelijk om binnen de hoedanigheden verschillende niveaus van bescherming na te streven voor gegevens die van zeer gevoelige aard zijn en gegevens die wat minder gevoelig van aard zijn.

De visie van de Rechtspraak op het gebied van privacy is hierna op visuele wijze weergegeven, waarbij op de verticale as de verscheidene soorten gegevensverwerkingen zijn weergegeven en op de horizontale as de categorie persoonsgegevens. Hoe dieper de kleur blauw, hoe zorgvuldiger de Rechtspraak om dient te gaan met de persoonsgegevens en hoe hoger het ambitieniveau zal zijn.

Figuur 2. Algemene visie

4.2 Aard van de gegevens

Zoals uit het voorgaande volgt, kunnen de open normen in de privacywetgeving – afhankelijk van de aard van de gegevens – op andere wijze geïnterpreteerd worden. Voor het onderscheid in gegevens, wordt aangesloten bij het onderscheid dat in de privacywetgeving wordt gemaakt.

Een persoonsgegeven wordt in de wet gedefinieerd als 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Een persoon wordt als identificeerbaar beschouwd indien hij direct of indirect kan worden geïdentificeerd aan de hand van één of meerdere gegevens, bijvoorbeeld voor- en achternaam, geboortedatum, woonadres, telefoonnummer, e-mailadres of IP-adres. Dit betekent dat zowel gegevens die over een persoon gaan, als gegevens die naar een natuurlijk persoon te herleiden zijn binnen de reikwijdte van de privacywetgeving vallen. Om te spreken van identificeerbaarheid is het niet noodzakelijk dat de naam van de persoon ook bekend is, als iemand uniek kan worden onderscheiden in een groep mensen, dan is deze persoon identificeerbaar en zijn de gegevens persoonsgegevens. Grofweg kan men ervan uit gaan dat alle gegevens die op een levend persoon betrekking hebben en het mogelijk maken om deze persoon (indirect) te identificeren – dan wel uniek te onderscheiden van andere personen – een persoonsgegeven zijn.[7]

Een aantal persoonsgegevens worden aangemerkt als gevoelige gegevens, dit zijn bijvoorbeeld financiële gegevens, het BSN, locatiegegevens, gegevens met betrekking tot kinderen of andere kwetsbare groepen. Nu deze gegevens in potentie meer bedreiging kunnen vormen voor de persoonlijke levenssfeer van betrokkenen, is het belangrijk om voor het verwerken van deze persoonsgegevens extra waarborgen te treffen om te garanderen dat ze in overeenstemming met de wet worden verwerkt.

Naast gewone en gevoelige persoonsgegevens, kent de privacywetgeving een strenger regime met betrekking tot bijzondere persoonsgegevens. Het uitgangspunt is dat voor het verwerken van bijzondere

[7] Art kel 4 lid 1 en overweging 26 en 30 AVG, art kel 3 lid 1 en overweging 21 Richtlijn; Art kel 29 Werkgroep (2007), Opinion 4/2007 on the Concept of Personal Data.

persoonsgegevens een verwerkingsverbod geldt. Als bijzondere persoonsgegevens worden onder meer gegevens aangemerkt die betrekking hebben op iemands godsdienst, ras, gezondheid, seksuele leven, politieke voorkeur, genetische gegevens en biometrische gegevens. Indien de beoogde verwerking echter onder een uitzondering valt, kan het verwerkingsverbod in sommige gevallen alsnog doorbroken worden.[8] Op grond van art. 10 AVG is de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen ook aan een apart regime onderworpen en mogen deze gegevens alleen worden verwerkt onder toezicht van de overheid of wanneer daarvoor een wettelijke basis bestaat en er voldoende waarborgen worden getroffen. De Richtlijn, alsmede de wetgeving waarin de Richtlijn geïmplementeerd zal worden regelt het wettelijk kader waaronder bevoegde autoriteiten strafrechtelijke persoonsgegevens mogen verwerken. De reden voor een strenger regime met betrekking tot voornoemde gegevens is gelegen in het feit dat de verwerking van bijzondere persoonsgegevens in potentie een grotere bedreiging vormt voor de persoonlijke levenssfeer van betrokkenen en aan de verwerking ervan voor de betrokkene bijzondere risico's kunnen zijn verbonden.[9] Bij de vaststelling of er in een bepaald geval sprake is van bijzondere persoonsgegevens, dient er niet alleen gekeken te worden naar de gegevens die direct betrekking hebben op een (mogelijk) bijzondere categorie, maar ook naar de gegevens waaruit de aanwezigheid van deze (mogelijke) categorie kan worden afgeleid. Wel is van belang dat er sprake is van een rechtstreeks verband: gegevens die hooguit een indicatie geven dat het om een (mogelijk) bijzondere categorie zou kunnen gaan, vallen buiten de reikwijdte van het strenge regime voor deze gegevens.[10]

4.3 Hoe gevoeliger de gegevens, hoe hoger de ambitie

Op basis van het hiervoor beschreven onderscheid, zal de Rechtspraak een hoger of lager ambitieniveau nastreven. Hoe gevoeliger de aard van de gegevens, hoe zorgvuldiger de Rechtspraak met deze gegevens om zal gaan. De Rechtspraak zal in het geval van verwerking van gevoelige en zeker bijzondere gegevens een hoog niveau van bescherming nastreven. Er zal bij de verwerking van deze gegevens veel aandacht zijn voor privacybescherming en er zullen te allen tijde voldoende waarborgen worden getroffen voor een zorgvuldige verwerking van deze gegevens, waarbij bijvoorbeeld gedacht moet worden aan het beveiligingsniveau dat gehanteerd wordt of de wijze waarop het kwaliteitsvereiste wordt ingevuld.[11] Hierna is het onderscheid schematisch weergegeven, waarbij geldt hoe donkerder de cirkel van kleur, hoe voorzichtiger de Rechtspraak omgaat met de persoonsgegevens.

[8] De uitzonderingen z jn opgesomd in art. 9 AVG (verdere uitwerking volgt in de uitvoeringswet AVG) en art. 10 Richtl jn (implementatie in Wpg en Wjsg).
[9] Overweging 51 AVG, overweging 37 Richtlijn
[10] Tekst en Commentaar Wet bescherming persoonsgegevens, p. 895
[11] Op grond van artikel 5 lid 1 sub c AVG en artikel 4 lid 1 sub c Richtlijn mogen persoonsgegevens slechts verwerkt worden voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

Figuur 3. Onderscheid soort gegevens

4.4 Geanonimiseerde gegevens

Op het moment dat persoonsgegevens volledig worden ontdaan van tot een persoon herleidbare aspecten kan er gesproken worden van geanonimiseerde data. Er zijn verschillende technieken waarmee gegevens geanonimiseerd kunnen worden, zoals aggregatie. Aggregatie beoogt te voorkomen dat een betrokkene wordt geïdentificeerd, dan wel uniek wordt onderscheiden van andere personen, door die samen te voegen met ten minste *n* andere personen.[12] Daartoe worden de gegevens op zodanige wijze gegeneraliseerd dat alle betrokkenen dezelfde waarde gemeen hebben.[13] Hierbij kan bijvoorbeeld worden gedacht aan het aantal maal dat in een bepaalde periode civiele zaken zijn gestart bij een bepaald arrondissement. Het is dan niet meer te achterhalen welke specifieke individuen in deze periode een zaak zijn gestart, maar alleen hoeveel mensen in totaal een civiele zaak zijn gestart in deze periode bij het betreffende arrondissement. Zodra gegevens volledig geanonimiseerd zijn, is de privacywetgeving niet langer van toepassing.[14]

Van belang hierbij is dat onder omstandigheden geanonimiseerde gegevens wel weer invloed kunnen hebben op de persoonlijke levenssfeer van betrokkenen. Zodra bijvoorbeeld geanonimiseerde data aan anderen wordt verstrekt of openbaar wordt gemaakt kan het, in combinatie met reeds bestaande gegevens, wel weer herleidbaar worden tot een persoon.
Daarnaast kunnen geaggregeerde gegevens ook een meer algemeen profiel vormen, die vervolgens weer op een persoon kan worden toegepast en daarmee consequenties kan hebben voor een individu. Voorts bestaat de mogelijkheid dat wanneer de waarde van *n* te klein is, een betrokkene alsnog geïdentificeerd, dan wel onderscheiden kan worden uit de groep betrokkenen.

Indien de Rechtspraak voor de uitvoering van innovatieve experimenten, maar bijvoorbeeld ook voor statistisch of wetenschappelijk onderzoek of mogelijk het verbeteren van de dienstverlening gebruik maakt van geanonimiseerde gegevens, dient er altijd goed in ogenschouw te worden genomen of het mogelijk is dat deze gegevens onder omstandigheden wel weer persoonsgegevens worden en de privacywetgeving gewoon van toepassing is. In samenspraak met de medewerkers die belast zijn met privacy binnen de Rechtspraak dient beoordeeld te worden of er in een specifiek geval gebruik gemaakt mag worden van geanonimiseerde gegevens en of er voorts daadwerkelijk sprake is van volledig anonieme gegevens.

[12] N ziet hierb j op het aantal personen waarmee de betrokkene wordt samengevoegd.
[13] Voor meer informatie zie: Artikel 29 Werkgroep (2014), Opinion 5/2014 on Anonymisation Techniques.
[14] Overweging 26 AVG, overweging 21 Richtlijn.

4.5 Relevante overwegingen

Naast de hoedanigheid waarin de Rechtspraak handelt en de aard van de gegevens zijn er tijdens de sessie nog een aantal overwegingen aangedragen waarmee rekening gehouden dient te worden bij de ontwikkeling van beleid van de Rechtspraak op het gebied van privacy.

4.5.1 Maatschappelijk belang

De Rechtspraak hecht er veel waarde aan om op een zorgvuldige wijze om te gaan met persoonsgegevens. Daar staat tegenover dat er door de Rechtspraak meerdere belangrijke maatschappelijke belangen in ogenschouw genomen dienen te worden. Zo heeft de Rechtspraak als staatsmacht ook een belangrijke functie om openbaarheid te betrachten richting de maatschappij. In sommige gevallen kan het voorkomen dat meerdere belangen, zoals openbaarheid van de rechtspraak en bescherming van de persoonlijke levenssfeer, een rol spelen en dat er een afweging dient te worden gemaakt tussen deze twee belangen. De nieuwe Europese privacywetgeving geeft de ruimte en handvaten voor deze – vaak complexe – belangenafweging. In (toekomstige) gevallen, wanneer een afweging gemaakt dient te worden tussen enerzijds de bescherming van de persoonlijke levenssfeer en anderzijds bijvoorbeeld openbaarheid, zal er – in samenspraak met de medewerkers die belast zijn met privacy binnen de Rechtspraak – te allen tijde een gedegen belangenafweging gemaakt dienen te worden en dient men ervoor zorg te dragen dat voldoende waarborgen worden getroffen om beide belangen te beschermen.

4.5.2 Innovatie

Naast het voorgaande, acht de Rechtspraak het tevens van belang dat zij bij ontwikkelingen aansluiten die spelen in de maatschappij en houdt de Rechtspraak – waar mogelijk – haar ogen open voor innovatie. Op het moment is er vanuit de Rechtspraak onder meer aandacht voor ontwikkelingen als big data en open data en wordt onderzocht of deze ontwikkelingen op een bepaalde wijze een rol kunnen spelen voor de Rechtspraak. Ook toekomstige ontwikkelingen zouden een rol kunnen gaan spelen voor de Rechtspraak. Bij het uitvoeren van experimenten met deze nieuwe technieken, spelen privacyaspecten een belangrijke rol. De Rechtspraak zal open staan voor het uitvoeren van dergelijke experimenten, maar zal bij het uitvoeren van dergelijke experimenten altijd zorgdragen dat de bescherming van de persoonlijke levenssfeer op juiste wijze wordt gewaarborgd. Het is derhalve van belang dat bij de opstart, ontwikkeling en uitrol van dergelijke experimenten altijd één van de medewerkers die belast is met privacy binnen de Rechtspraak wordt betrokken, die de in onderhavig document geformuleerde visie op het gebied van privacy in acht zal nemen. Bij dergelijke experimenten dient te allen tijde goed onderzocht te worden welke gegevens wel en welke gegevens niet verstrekt kunnen worden, dan wel betrokken kunnen worden bij dergelijke experimenten. Waar mogelijk zal de Rechtspraak voor de uitvoering van dergelijke experimenten gebruik maken van geanonimiseerde gegevens (zie 4.3). Indien het in sommige gevallen niet mogelijk is gebruik te maken van geanonimiseerde gegevens, zal er altijd voor gezorgd moeten worden dat er – afhankelijk van de aard van de gegevens – voldoende waarborgen worden getroffen teneinde de privacy te beschermen. Experimenten die uitgevoerd worden door de Rechtspraak, dan wel experimenten waarbij de Rechtspraak als belanghebbende aansluit, dienen te allen tijde in overeenstemming met de privacywetgeving te worden uitgevoerd.

4.6 Actiepunten

De medewerkers die belast zijn met privacy binnen de Rechtspraak[15] dienen de hierboven geformuleerde visie te vertalen naar de door de privacywetgeving gestelde normen. Voornoemde medewerkers dienen daarnaast de vervolgstappen, concrete actiepunten, vorm te geven. De concrete actiepunten zijn in bijlage I op schematische wijze gevoegd bij dit strategisch plan. Het is aan deze medewerkers, om aan de hand van de geformuleerde visie prioritering aan te brengen in de actiepunten, de normenkaders en richtlijnen te ontwikkelen en het bewustzijn te creëren.

Een belangrijk punt waarmee voornoemde medewerkers rekening dienen te houden is dat wegens de aard van de organisatie, binnen de Rechtspraak al veel waarde wordt gehecht aan een zorgvuldige omgang met zaakgegevens van betrokken partijen. Rechters en medewerkers van de Rechtspraak zijn zich bewust van de – mogelijk – gevoelige aard van zaakgegevens en gaan hier op vertrouwelijke en integere wijze mee om. Bij de inbedding van de privacywetgeving zal zo veel mogelijk dienen te worden voortgeborduurd op en aangesloten worden bij deze reeds bestaande zorgvuldige omgang. Voorkomen dient te worden dat het privacy beleid zo omvattend wordt ingericht dat binnen de Rechtspraak een grote hoeveelheid (procedurele) veranderingen en nieuwe regelgeving wordt ingevoerd. Er dient aangesloten te worden bij het bestaande bewustzijn en bestaande processen en procedures, zodat de aankomende nieuwe wetgeving op zo gestructureerd mogelijke wijze wordt ingebed in de organisatie. Het is van belang dat bij de inbedding van de privacywetgeving rechters en medewerkers van de Rechtspraak zo min mogelijk worden belemmerd in de uitvoering van hun werkzaamheden.

Daarnaast dienen de medewerkers die verantwoordelijk zijn voor privacy binnen de Rechtspraak in ogenschouw te nemen dat er niet uitsluitend aandacht besteedt dient te worden aan de gedigitaliseerde systemen van de Rechtspraak en aan de ontwikkeling van nieuw beleid, maar dat ook de huidige processen en procedures herijkt dienen te worden. Hierbij zal het onder meer ook nog gaan om processen en procedures omtrent fysieke dossierstukken. Het is derhalve van belang dat de medewerkers die verantwoordelijk zijn voor het privacy beleid ook de aanpassing van huidige processen en procedures meenemen bij de implementatie van de wetgeving.

[15] Waar wordt gesproken over medewerkers die verantwoordelijk zijn voor privacy binnen de Rechtspraak, wordt gedoeld op de medewerkers die belast zijn of worden met de ontwikkeling en implementatie van de normenkaders en richtlijnen met betrekking tot privacy binnen de Rechtspraak, alsmede de medewerkers die na het van toepassing worden van de aankomende privacywetgeving belast blijven met privacy binnen de Rechtspraak.

5 Beleggen rollen en verantwoordelijkheden

Een belangrijk tweede onderdeel van het inrichten van een privacy beleid is het beleggen van de rollen en verantwoordelijkheden. Het is van belang om helder voor ogen te hebben waar de verantwoordelijkheden voor privacy binnen de Rechtspraak worden belegd, zodat op gestructureerde wijze uitvoering wordt gegeven aan privacy en het risico op non-compliance wordt verminderd. Tijdens de bijeenkomst is daarom tevens gesproken over het beleggen van een aantal rollen en verantwoordelijkheden. Gelet op de aankomende privacywetgeving en de nieuwe wettelijke vereisten die daarin worden geïntroduceerd, is het van belang dat op korte termijn besloten wordt op welke wijze de verantwoordelijkheden worden belegd, zodat spoedig aan de slag gegaan kan worden met de implementatie van de wetgeving.

5.1 Algemene uitkomsten

Zoals uit het voorgaande (zie 4.6) reeds naar voren is gekomen dient de privacywetgeving zo gestructureerd mogelijk ingebed te worden binnen de Rechtspraak, zodat rechters en medewerkers van de Rechtspraak zo min mogelijk belemmerd worden in hun werkzaamheden. Gelet hierop en gelet op het feit dat een groot gedeelte van het privacy beleid nog ontwikkeld dient te worden en getracht wordt de gerechten zo min mogelijk te belasten met de ontwikkeling hiervan, is tijdens de bijeenkomst de voorkeur uitgesproken om de verantwoordelijkheid voor de inrichting van het privacy beleid landelijk – bij de Raad – te beleggen. Met de komst van het programma KEI en de KEI-wetgeving, wordt binnen de Rechtspraak een grote slag gemaakt op het gebied van digitalisering. Op grond van artikel 91 Wet op de rechterlijke organisatie zorgt de Raad voor ondersteuning van de bedrijfsvoering van de gerechten in het bijzonder gericht op automatisering en bestuurlijke informatievoorziening. Door de invoering van KEI zal het er steeds meer naar toe gaan dat de gegevens van de Rechtspraak worden opgeslagen in één centraal systeem met één centrale dataopslag. De ontwikkeling en het beheer van deze digitale systemen wordt uitgevoerd door de landelijke dienst, Spir-it. Ieder gerechtsbestuur is echter wel verantwoordelijk voor de juistheid van de gegevens die worden verwerkt in de zaaksdossiers die bij dat betreffende gerecht aanhangig zijn gemaakt. Dat betekent dat er een gezamenlijke verantwoordelijkheid is voor de gegevensverwerkingen in de centrale digitale systemen van de Rechtspraak: te weten de Raad en de gerechtsbesturen.[16] De Raad en de gerechtsbesturen bepalen gezamenlijk het doel van en de middelen voor de gegevensverwerkingen van de Rechtspraak in de digitale systemen en zijn daarmee verwerkingsverantwoordelijke in de zin van de privacywetgeving. De vereisten die voortvloeien uit de AVG en de Richtlijn zijn opgelegd aan de verwerkingsverantwoordelijke.
Gelet op het feit dat er in de digitale systemen sprake is van een gezamenlijke verantwoordelijkheid tussen Raad en gerechten, is in de strategiesessie de wens geuit de verantwoordelijkheid voor de inrichting van het privacy beleid landelijk te beleggen. De privacywetgeving ziet niet uitsluitend op de gedigitaliseerde systemen van de Rechtspraak, maar ziet tevens op de huidige processen en procedures. Hierbij gaat het veelal ook nog om processen en procedures omtrent fysieke dossierstukken. Gelet hierop, zullen ook deze processen en procedures mee worden genomen in de ontwikkeling en implementatie van het privacy beleid, dat landelijk belegd zal worden.
Voor de inbedding van het privacy beleid dient aansluiting te worden gezocht bij de wijze waarop informatiebeveiliging thans is ingebed in de organisatie.[17] Aansluitend bij de huidige situatie en de wijze waarop informatiebeveiliging thans is ingeregeld, zal er één FG aangesteld worden voor de gehele Rechtspraak.[18] De FG zal gepositioneerd zijn bij de Raad en zal – middels normenkaders en richtlijnen

[16] Privacykader digitaal procederen in het Civiele en Bestuursrecht (KEI), Raad voor de rechtspraak, 16 april 2015, p. 4
[17] Het beveiligingsbeleid binnen de Rechtspraak kenmerkt zich door één landelijk beveiligingsambtenaar, alsmede een plaatsvervangend beveiligingsambtenaar, die gepositioneerd zijn b j de Raad. Bij de Raad is tevens een CISO gepositioneerd. Eén van de leden Raad is eindverantwoordelijke en heeft beveiliging in zijn portefeuille zitten. Ieder gerecht heeft een beveiligings- en veiligheidscoördinator aangesteld en binnen de landelijke diensten z jn ook verantwoordelijken voor beveiliging aangewezen. Voornoemde verantwoordelijken komen bij tijd en wijlen samen in een landelijk overleg, genaamd het Lobro.
[18] Op grond van artikel 37 lid 4 AVG en artikel 32 lid 3 Richtlijn is het mogel jk om één FG voor de gehele Rechtspraak aan te stellen: 'Wanneer de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie of overheidsorgaan is, kan één

– adviseren en informeren omtrent de verplichtingen die voortvloeien uit de privacywetgeving en een belangrijke rol spelen bij het toezicht op de naleving van de wetgeving. De FG heeft de functie om Raad, gerechten en landelijke diensten van advies te voorzien en heeft een adviserende rol op onder meer het gebied van PIA's *('privacy impact assessment')*.[19] Daarnaast heeft de FG de bevoegdheid om Raad, gerechten en landelijke diensten er op te wijzen als er niet in overeenstemming met de privacywetgeving wordt gehandeld. De FG moet dan ook in staat worden gesteld om op eenvoudige wijze te kunnen schakelen en verslag uit te kunnen brengen aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, te weten het lid van de Raad, die privacy in portefeuille heeft, en/of de besturen van de gerechten. Indien gerechten of landelijke diensten op structurele wijze niet voldoen aan de privacywetgeving, zal er voor zowel FG als het lid van de Raad, die privacy in portefeuille heeft, een rol zijn weggelegd om te escaleren richting bestuur van gerechten en directie van landelijke diensten. De FG dient er derhalve op toe te zien dat de AVG en de Richtlijn nageleefd wordt. Dit betekent echter niet dat de FG verantwoordelijk gehouden kan worden wanneer niet in overeenstemming met de wetgeving wordt gehandeld. De verwerkingsverantwoordelijke, te weten de Raad en/of gerechten, blijven te allen tijde eindverantwoordelijke voor de naleving van de vereisten die voortvloeien uit de AVG en de Richtlijn.

Om op adequate wijze uitvoering te geven aan de privacywetgeving is tijdens de sessie tevens aangegeven dat het nodig is een privacy officer aan te stellen bij Spir-it en LDCR. Gezien de werkzaamheden die Spir-it uitvoert en de diensten die zij leveren, ligt het zwaartepunt van de privacyvraagstukken bij Spir-it.[20] Het wordt dan ook raadzaam geacht de privacy officer bij Spir-it te positioneren en onder de verantwoordelijkheid van Spir-it te laten vallen. De privacy officer zal naar verwachting het merendeel van zijn werkzaamheden voor Spir-it verrichten, maar zal tevens in staat moeten worden gesteld privacyvraagstukken op te vangen van het LDCR. Door de aanstelling van een privacy officer wordt in een vroeg stadium bij de business en ontwikkeling aandacht besteedt aan de vereisten die voortvloeien uit de privacywetgeving en kunnen er waar nodig meteen aanpassingen worden doorgevoerd om overeenstemming te bereiken met de privacywetgeving. Van belang is dat de privacy officer niet is belast met de taken zoals deze in de AVG en Richtlijn zijn toegekend aan de FG en dan ook het toezien op de naleving van de wetgeving binnen de organisatie. De privacy officer kan zich wel te allen tijde voor advies wenden tot de FG.

De wijze waarop de verantwoordelijkheid voor privacy op dit moment binnen SSR is belegd, zal niet worden aangepast. Dat betekent dat het SSR een aanspreekpunt privacy heeft die uitvoering geeft aan de landelijk opgestelde richtlijnen en normenkaders en binnen SSR vraagstukken opvangt omtrent privacy. Het aanspreekpunt privacy binnen SSR kan zich uiteraard te allen tijde wenden tot de FG voor advies.

Om de gerechten zo min mogelijk te belasten met de implementatie van de aankomende privacywetgeving, zullen de verantwoordelijkheden voor privacy binnen de gerechten tevens niet worden herbelegd. De wijze waarop privacy thans is ingericht binnen de gerechten zal dan ook worden voortgezet. Dat betekent dat de gerechten een aanspreekpunt privacy hebben, in het merendeel van de gevallen zal dit de beveiligings- en veiligheidscoördinator zijn ('BVC-er'), waarmee de FG contact kan opnemen omtrent kwesties rondom privacy. De aanspreekpunten privacy zijn verantwoordelijk voor de privacyvraagstukken die spelen binnen het betreffende gerecht en dienen uitvoering te geven aan de

functionaris voor gegevensbescherming worden aangewezen voor verschillende dergelijke instanties of organen, met inachtneming van hun organisatiestructuur en omvang.'

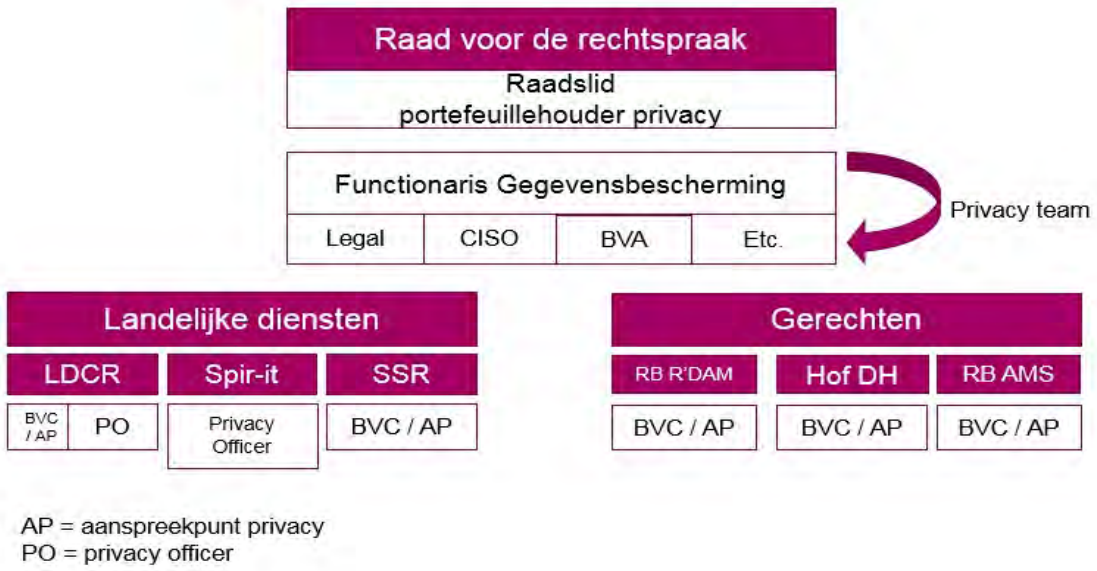
[19] Indien een verwerking waarschijnlijk gepaard gaat met hoge risico's in verband met de rechten en vr jheden van natuurlijke personen, dient een PIA te worden uitgevoerd. Een PIA dient ten minste een algemene beschrijving van de beoogde verwerkingen, een beoordeling van de risico's voor de rechten en vr jheden van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen en aan te tonen dat aan de AVG en de Richtl jn wordt voldaan, met inachtneming van de rechten en legitieme belangen van de betrokkenen en andere betrokken personen. artikel 35 AVG, artikel 27 Richtl jn.

[20] Op basis van de aangedragen opmerkingen van de directeur LDCR en medewerkers van Spir-it op het concept strategisch privacy plan, is de conclusie getrokken dat het zwaartepunt van het aantal privacyvraagstukken bij Spir-it ligt.

landelijk opgestelde normenkaders en richtlijnen binnen hun betreffende gerecht. De aanspreekpunten privacy kunnen zich te allen tijde tot de FG wenden om advies in te winnen. Het wordt ten zeerste aangeraden om bij de gerechten de mogelijkheden te onderzoeken of per locatie een aanspreekpunt privacy kan worden aangewezen. Sinds de herziening van de gerechtelijke kaart zijn het aantal arrondissementen en daarmede het aantal rechtbanken verminderd. Deze rechtbanken zijn weer verdeeld over een viertal ressorten; voorheen waren dit er vijf. Om een locatie van een gerecht zo goed mogelijk te kunnen ondersteunen bij de vraagstukken op het gebied van privacy, wordt het ten zeerste aanbevolen om bij elke locatie een aanspreekpunt privacy aan te wijzen. Dat betekent dat er bijvoorbeeld bij het gerechtshof Arnhem – Leeuwarden zowel een aanspreekpunt privacy in Arnhem als Leeuwarden aangesteld moet worden, zodat er per locatie één medewerker is die binnen de betreffende locatie goed zicht heeft op hetgeen zich binnen deze locatie allemaal afspeelt. Hierdoor is het aanspreekpunt privacy in staat de vraagstukken van de betreffende locatie adequaat af te handelen en uitvoering te geven aan de opgestelde normenkaders en richtlijnen met betrekking tot privacy. Door bij iedere locatie een aanspreekpunt privacy aan te stellen wordt de FG tevens in staat gesteld om eenvoudig te schakelen met het aanspreekpunt privacy omtrent privacyvraagstukken die voorvallen binnen de betreffende locatie. Om uniformiteit binnen het betreffende gerecht te kunnen borgen is het uiteraard van belang dat de aanspreekpunten privacy onderling nauw met elkaar samenwerken en op eenvoudige wijze met elkaar in contact kunnen treden. Op welke wijze hieraan uitvoering wordt gegeven, dient op bestuurlijk niveau door de gerechten zelf vormgegeven te worden.

Gelet op het voorgaande, laat de verdeling van de verantwoordelijkheden binnen de Rechtspraak op het gebied van privacy zich op visuele wijze het best als volgt weergeven, waarbij de grootte van de rechthoek aangeeft welk gewicht de functie heeft. Hierbij dient opgemerkt te worden dat deze visualisatie uitsluitend ziet op het beleggen van de verantwoordelijkheden op het gebied van privacy en slechts een weergave is van de compliance structuur waar tijdens de strategiesessie de voorkeur voor uit is gesproken. De compliance structuur kan te allen tijde aangepast worden, alsmede het gewicht dat toebedeeld is aan een bepaalde functie.

Figuur 4. Rollen en verantwoordelijkheden



* de drie gerechten zoals genoemd in de visualisatie zijn opgesomd ter illustratie. De verantwoordelijkheidsverdeling ziet op alle gerechten die onderdeel zijn van de Rechtspraak.

Al enige tijd wordt een maandelijkse bijeenkomst gehouden onder de naam privacy expertgroep.[21] Nadat de rollen en verantwoordelijkheden zijn (her)belegd, zal opnieuw gekeken moeten worden op welke wijze invulling gegeven zal worden aan de privacy expertgroep en van welke medewerkers het raadzaam wordt geacht daarbij aanwezig te zijn, dan wel als agenda lid deel te nemen, waarbij zowel gerechten, landelijke diensten als Raad vertegenwoordigd dienen te worden. In deze bijeenkomst zullen vraagstukken omtrent de interpretatie van het privacy beleid van de Rechtspraak behandeld worden, alsmede allerhande privacyvraagstukken die spelen binnen de organisatie.

5.2 De rol van FG

Binnen de Rechtspraak is er reeds enige jaren een FG aangesteld. De FG is gepositioneerd bij de Raad. De FG heeft thans – naast de andere functie die door de FG wordt vervuld – een beperkt aantal uren per week om de functie van FG uit te voeren. Onder de aankomende wetgeving, krijgt de FG echter een meer omvattende rol toebedeeld dan onder de huidige wet.

5.3 Wettelijke vereisten FG

Onder de nieuwe wetgeving wordt het onder meer voor overheidsinstanties verplicht om een FG aan te stellen.[22] De FG gaat een belangrijke rol spelen bij de inbedding van de privacywetgeving en het creëren van een gegevensbeschermingscultuur binnen de organisatie. De FG dient er daarnaast op toe te zien dat de AVG en de Richtlijn binnen de organisatie worden nageleefd. In de AVG zijn de wettelijke vereisten omtrent de instelling, middelen en taken van de FG vastgelegd in de artikelen 37 tot en met 39 en in de Richtlijn in de artikelen 32 tot en met 34. De FG wordt aangewezen op grond van zijn / haar professionele kwaliteiten, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen om de aan de FG toebedeelde taken te vervullen.[23]

5.3.1 Middelen

Op grond van de AVG en de Richtlijn dient de FG naar behoren en tijdig te worden betrokken bij alle aangelegenheden die verband houden met de bescherming van de persoonsgegevens. Om zijn taken te vervullen dient de FG toegang te verkrijgen tot persoonsgegevens en verwerkingsactiviteiten die verricht worden door de verantwoordelijke. Aan de FG dienen voldoende middelen beschikbaar gesteld te worden, zodat hij zijn taken naar behoren kan vervullen en zijn deskundigheid in stand kan houden. De FG moet in staat worden gesteld de taken en verplichtingen onafhankelijk te vervullen. Dat betekent dat de FG geen instructies mag ontvangen met betrekking tot de uitvoering van zijn taken, zoals bijvoorbeeld het te bereiken resultaat. De FG mag daarnaast geen instructies ontvangen om een bepaald standpunt in te nemen over een gegevensbeschermingskwestie, bijvoorbeeld over de wettelijke interpretatie. De FG moet echt in staat worden gesteld om zijn werkzaamheden onafhankelijk te verrichten en mag dan ook niet ontslagen of gestraft worden voor de uitvoering van zijn of haar taken. De naleving van de wettelijke vereisten die voortvloeien uit de privacywetgeving blijft een verantwoordelijkheid van de verwerkingsverantwoordelijke zelf, te weten de Raad en/of gerechten en niet van de FG. De FG kan – naast de werkzaamheden die worden verricht als zijnde FG – nog andere taken en plichten vervullen. Deze taken en plichten mogen echter niet tot een belangenconflict leiden met de taken van de FG. Van belangenverstrengeling kan onder meer sprake zijn wanneer de FG binnen de organisatie ook een functie heeft waarin hij of zij het doel en de middelen van een

[21] De aanwezigen bij de huidige privacy expertgroep zijn de FG (gepositioneerd bij de Raad), de CISO (gepositioneerd bij de Raad), de adviseurs recht en ICT (gepositioneerd bij de Raad), de security officer (gepositioneerd bij Spir-it), de Unitmanager afdeling AK & S (gepositioneerd b j Spir-it).
[22] Hierbij dient opgemerkt te worden dat de gerechten b j de uitoefening van hun gerechtel jke taken uitgezonderd worden van de verplichting een FG aan te stellen. Deze uitzondering ziet er voornamelijk op dat de FG geen beslissingen mag nemen die de onafhankel jkheid van de rechter in gevaar kan brengen. Deze uitzondering ziet uitsluitend op de gerechten wanneer zij gerechtelijke taken uitvoeren. Het wordt de Rechtspraak in zijn geheel op grond van de AVG en de Richtl jn dan ook wel ten zeerste aangeraden een FG aan te stellen conform de vereisten zoals vastgelegd in deze wetgeving.
[23] Artikel 37 lid 5 AVG, artikel 32 lid 2 Richtl jn.

gegevensverwerking bepaalt, denk hierbij onder meer aan een managementpositie zoals hoofd financiën, strategie, marketing, IT of HRM.[24]

5.3.2 Taken

Op grond van de AVG en de Richtlijn zal de FG verantwoordelijk zijn voor alles wat te maken heeft met de bescherming van persoonsgegevens binnen de organisatie. De FG informeert en adviseert bijvoorbeeld over de verplichtingen die de verwerkingsverantwoordelijke en zijn werknemers hebben op grond van de privacywetgeving, ziet toe op naleving van de wetgeving, met inbegrip van de toewijzing van verantwoordelijkheden, bewustwording en opleiding van de bij de verwerking betrokken medewerkers, creëert bewustwording in de gehele organisatie en ziet toe op de uitvoering daarvan en werkt samen met de AP en treedt op als contactpersoon voor de AP.[25]

Daar komt bij dat de AP niet bevoegd is om toezicht te houden op de verwerking van persoonsgegevens door gerechten in het kader van hun gerechtelijke taken. Dit teneinde de onafhankelijkheid van de rechterlijke macht bij de uitoefening van haar rechterlijke taken, waaronder besluitvorming, te waarborgen. Let wel deze uitzondering dient strikt gelezen te worden en ziet uitsluitend op gegevensverwerkingen die de onafhankelijkheid van de rechter in gevaar kunnen brengen. Het toezicht op die gegevensverwerkingen moet worden toevertrouwd aan specifieke instanties binnen de rechterlijke organisatie, die met name de naleving van de regels van de AVG en Richtlijn moeten garanderen, leden van de rechterlijke macht van hun verplichtingen op grond van de privacywetgeving sterker bewust moeten maken, en klachten met betrekking tot gegevensverwerkingen moeten behandelen.[26] Het is goed denkbaar dat het merendeel van voornoemde taken voor rekening van de FG komen.

De FG dient bij de uitvoering van de taken naar behoren rekening te houden met de aan verwerkingen verbonden risico's en met de aard, de omvang, de context en de verwerkingsdoeleinden. Opgemerkt dient te worden dat de gerechten en de Raad te allen tijde verantwoordelijk blijven voor de naleving van de vereisten die voortvloeien uit de AVG en richtlijn. De FG zal niet persoonlijk verantwoordelijk zijn wanneer wettelijke vereisten uit de AVG en Richtlijn niet worden nageleefd. De verwerkingsverantwoordelijke, te weten de Raad en/of gerechten, zijn degene die er uiteindelijk op toe dienen te zien en moeten kunnen aantonen dat zij voldoen aan de vereisten uit de AVG en de Richtlijn. De FG zal de Raad, gerechten en landelijke diensten – middels normenkaders en richtlijnen – informeren en adviseren omtrent de vereisten die voortvloeien uit de wetgeving en houdt voorts ook toezicht op de naleving van de wetgeving. De normenkaders en richtlijnen die de FG opstelt omtrent de wettelijke verplichtingen die voortvloeien uit de wetgeving zal de FG – naar eigen inzicht – voorleggen aan het lid van de Raad, die privacy in portefeuille heeft, en de besturen van de gerechten.
De verwerkingsverantwoordelijke, te weten Raad en/of gerechten, dienen er uiteindelijk zelf voor te zorgen dat de wetgeving in de organisatie ook daadwerkelijk wordt nageleefd.

Zoals uit het voorgaande blijkt zal de FG dus een belangrijke rol spelen bij het adviseren en informeren – middels normenkaders en richtlijnen – omtrent de verplichtingen die voortvloeien uit de wetgeving en bij het creëren van bewustwording rondom privacy. Om het beleid zo gestructureerd mogelijk te implementeren, is het echter wel van belang dat binnen de gerechten en landelijke diensten op bestuurlijk niveau draagvlak is voor privacy en dat binnen gerechten en landelijke diensten ook gewerkt wordt, bijvoorbeeld door de BVC-ers, dan wel aanspreekpunten privacy en de privacy officer, aan bewustwording onder medewerkers. Om privacy zo goed mogelijk in te bedden in de Rechtspraak, dient

[24] Artikel 38 AVG, artikel 33 Richtlijn. Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg#faq
[25] Artikel 39 AVG, artikel 34 Richtlijn.
[26] Artikel 55 lid 3 AVG en overweging 20, art kel 45 lid 2 en overweging 80 Richtlijn.

het belang van privacy op bestuurlijk niveau te worden erkend en naar de medewerkers te worden uitgedragen.

5.4 Uitbreiden rol FG

Zoals hiervoor aangegeven is er reeds een FG aangesteld bij de Rechtspraak. Deze functie wordt thans, naast de functie van Senior Juridisch Adviseur, voor een beperkt aantal uren per week vervuld. De FG is op dit moment gepositioneerd bij de Raad. Er is door de FG binnen de Rechtspraak al hard gewerkt aan de implementatie van de huidige Wbp en aan het creëren van bewustwording omtrent privacy. Op grond van de aankomende wetgeving en op grond van uitkomsten van de strategiesessie zal het takenpakket van de FG echter aanzienlijk uitgebreid worden en zal de rol van de FG in zwaarte toenemen. Dat betekent dat de huidige invulling niet voldoende zal zijn om naar behoren en op adequate wijze uitvoering te geven aan de wettelijke vereisten uit de AVG en de Richtlijn. Tijdens de strategiesessie is derhalve besloten dat op termijn – in samenspraak met de huidige FG – vormgegeven moet worden op welke wijze invulling gegeven zal worden aan de nieuwe FG functie, zodat de FG functie op 25 mei 2018 in overeenstemming is met de wettelijke vereisten zoals neergelegd in de artikelen 37 – 39 AVG en de artikelen 32 – 34 Richtlijn (zie 5.3).

Nu er voorafgaand aan de implementatietermijn van de aankomende privacywetgeving nog een aanzienlijk aantal actiepunten en verbeteringen dienen te worden doorgevoerd, wordt het ten zeerste aangeraden om zo spoedig mogelijk op projectbasis een privacyspecialist aan te stellen, dan wel in te huren die het project rondom de implementatie van de aankomende privacywetgeving zal begeleiden en uitvoeren. Deze privacyspecialist zal fungeren als projectleider en zal zich bezig houden met het opstellen van normenkaders en richtlijnen. Tijdens de implementatietermijn dient dan nader gekeken te worden hoe de huidige rol van FG uitgebreid zal gaan worden, zodat de Rechtspraak op 25 mei 2018 over een FG beschikt die in staat is de taken uit te voeren zoals deze zijn neergelegd in de wetgeving.

5.5 Aanstelling privacy officer Spir-it

Om op adequate wijze uitvoering te kunnen geven aan de privacywetgeving, is tijdens de sessie aangegeven – zoals in 5.1 reeds vermeld – dat het nodig wordt geacht een privacy officer aan te stellen bij Spir-it en LDCR. Gezien de werkzaamheden die Spir-it uitvoert en de diensten die zij leveren, ligt het zwaartepunt van de privacyvraagstukken bij Spir-it. Het wordt dan ook raadzaam geacht de privacy officer bij Spir-it te positioneren en onder verantwoordelijkheid van Spir-it te laten vallen. De privacy officer zal naar verwachting het merendeel van zijn werkzaamheden voor Spir-it uitvoeren, maar dient daarnaast ook in staat te worden gesteld om privacyvraagstukken van het LDCR op te vangen. Op bestuurlijk niveau dient besloten te worden op welke wijze de verdeling van de werkzaamheden tussen Spir-it en LDCR concreet vormgegeven zal worden. Met het oog op de aankomende IV-organisatie is het mogelijk dat de positionering van de privacy officer te zijner tijd wordt herzien. Dit is echter afhankelijk van de uiteindelijke invulling van de IV-organisatie en dient in een later stadium beoordeeld te worden.

De privacy officer vervult een andere rol dan de FG en hoeft dan ook niet te voldoen aan de wettelijke vereisten zoals deze in de AVG en de Richtlijn zijn opgelegd aan de FG (zie 5.3). Wel is het van belang een privacy officer aan te stellen die deskundig is op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. De privacy officer zal zich onder meer bezig houden met de operationalisering van beleid binnen Spir-it en de landelijk opgestelde normenkaders en richtlijnen vertalen naar concrete maatregelen voor de ICT voorzieningen die door Spir-it worden beheerd en ontwikkeld.
De privacy officer ondervangt daarnaast in een vroeg stadium van de ontwikkeling al vele operationele vraagstukken, speelt een begeleidende rol bij het uitvoeren van PIA's, denkt mee over de mogelijke privacy aspecten die spelen bij de ontwikkeling van nieuwe producten en diensten, speelt een belangrijke rol bij het in kaart brengen van gegevensverwerkingen, begeleidt de operationalisering

rondom nieuwe experimenten zoals big data e.d., lost allerhande ad hoc privacy vraagstukken op die spelen rondom KEI en creëert bewustwording onder medewerkers. Door het aanstellen van een privacy officer bij Spir-it wordt in een vroeg stadium al veel aandacht besteed aan de vereisten die voortvloeien uit de privacywetgeving en kunnen er – waar mogelijk – al veel aanpassingen worden doorgevoerd om overeenstemming met de privacywetgeving te bereiken. Dit zal het werkproces meer gestructureerd maken en uiteindelijk sneller laten verlopen.

Het wordt raadzaam geacht de privacy officer tevens een aantal van voornoemde werkzaamheden voor het LDCR uit te laten voeren, dan wel een begeleidende rol te laten spelen bij de uitvoering van deze werkzaamheden. Daarnaast dient de privacy officer tevens in staat te worden gesteld om privacyvraagstukken van het LDCR op te vangen. Nu het in de lijn der verwachting ligt dat de privacy officer het merendeel van zijn werkzaamheden voor Spir-it zal verrichten, wordt het LDCR wel aangeraden hun aanspreekpunt privacy te behouden. Het aanspreekpunt privacy kan dan – onder begeleiding van de privacy officer – binnen het LDCR uitvoering geven aan de landelijk opgestelde normenkaders en richtlijnen met betrekking tot privacy. Tevens kan het aanspreekpunt privacy operationele privacyvraagstukken binnen het LDRC afvangen die meer van organisatorische aard zijn, zoals vraagstukken die te maken hebben met de meldplicht datalekken. Het wordt echter wel ten zeerste aangeraden de privacy officer te betrekken bij privacyvraagstukken die voortvloeien uit de ‘core business’ van het LDCR; dus onder meer vraagstukken omtrent projecten die door het LDCR worden uitgevoerd, dan wel vooronderzoeken die door het LDCR worden uitgevoerd.

Van belang is dat de functie van de privacy officer los gezien dient te worden van de rol van de FG. De FG zal de taken vervullen zoals deze zijn neergelegd in de AVG en de Richtlijn en ziet toe op de naleving van de wetgeving binnen de Rechtspraak. De FG is degene die te allen tijde extern de contactpersoon zal zijn als het aankomt op zaken die spelen rondom privacy.
De privacy officer zal – zoals hiervoor reeds vermeld – verantwoordelijk zijn voor de operationalisering binnen Spir-it en, waar nodig LDCR, en zal de landelijke opgestelde normenkaders en richtlijnen vertalen naar concrete maatregelen. De privacy officer ondervangt daarnaast de privacyvraagstukken waar medewerkers van Spir-it en LDCR in de uitvoering van hun werkzaamheden tegen aan lopen. Indien de privacy officer aanvullende vragen heeft of advies nodig heeft over de interpretatie van de wetgeving of de normenkaders en richtlijnen, kan hij of zij zich te allen tijde wenden tot de FG. De FG zal daarnaast advies uitbrengen aan de privacy officer over de PIA’s die door hem of haar zijn uitgevoerd. De FG heeft daarnaast de bevoegdheid in te grijpen op het moment dat de wetgeving en normenkaders en richtlijnen niet op juiste wijze worden nageleefd. De privacy officer zal echter niet onder rechtstreeks gezag van de FG vallen. Zoals reeds hiervoor vermeld zal de privacy officer worden gestationeerd bij Spir-it en onder de verantwoordelijkheid van Spir-it vallen.

Er is daarnaast geen sprake van een aansturende rol vanuit de privacy officer naar de aanspreekpunten privacy (het merendeel de BVC-ers) bij de gerechten en SSR. De privacy officer is verantwoordelijk voor het operationaliseren van de normenkaders en richtlijnen binnen Spir-it, en mogelijk LDCR, en voor de privacyvraagstukken waar de medewerkers binnen Spir-it en LDCR in hun werkzaamheden tegen aan lopen. De privacy officer draagt deze verantwoordelijkheid niet ten aanzien van de gerechten en het SSR. Het wordt echter wel aangeraden de privacy officer en aanspreekpunten privacy eenvoudig met elkaar te kunnen laten schakelen omtrent overlappende privacyvraagstukken en teneinde advies bij elkaar in te kunnen winnen.

5.6 Actiepunten

Tijdens de strategiesessie zijn er een aantal beslissingen genomen omtrent het beleggen van de verantwoordelijkheden op het gebied van privacy. In navolging daarvan, is het van belang dat deze verantwoordelijkheden op zo kort mogelijke termijn op juiste wijze worden belegd. Hierbij wordt het ten zeerste aangeraden om zo spoedig mogelijk op projectbasis een privacyspecialist aan te stellen, dan wel in te huren die het project rondom de implementatie van de aankomende privacywetgeving gaat begeleiden en uitvoeren. Daarnaast het wordt het aanbevolen om op termijn – in samenspraak met de huidige FG – te bepalen op welke wijze de functie van FG ingericht zal worden, zodat de Rechtspraak op 25 mei 2018 over een FG beschikt die voldoet aan de vereisten die voortvloeien uit de AVG en Richtlijn. Het wordt tevens raadzaam geacht om op korte termijn een privacy officer aan te stellen bij Spir-it en LDCR. Op bestuurlijk niveau dient spoedig te worden bepaald op welke wijze de verdeling van de werkzaamheden tussen Spir-it en LDCR concreet vormgegeven gaat worden.
Zodra deze actiepunten zijn doorgevoerd, dan wel een start is gemaakt met deze actiepunten, kan de visie door de medewerkers die belast zijn met het privacy binnen de Rechtspraak vertaald worden naar de door de privacywetgeving gestelde normen en kan vorm worden gegeven aan de vervolgstappen.

6 Conclusie

Om op 25 mei 2018 in overeenstemming te handelen met de aankomende privacywetgeving, waaronder de AVG en de Richtlijn, alsmede privacy op structurele wijze in te bedden in de Rechtspraak, heeft er op bestuurlijk niveau een strategiesessie plaatsgevonden bij de Raad. In onderhavig plan zijn de uitkomsten van deze sessie uiteengezet, waarin beslissingen zijn genomen omtrent de algemene visie van de Rechtspraak op het gebied van privacy en omtrent het beleggen van de verantwoordelijkheden op het gebied van privacy.

Visie

De Rechtspraak acht het van belang om op zorgvuldige wijze met de privacy en persoonlijke gegevens van betrokkenen om te gaan, waarbij het zowel gaat om gegevens van betrokkenen die verwerkt worden ten behoeve van het primaire proces (hieronder vallen tevens gegevensverwerkingen gerelateerd aan het primaire proces) als gegevens van medewerkers van de Rechtspraak. Het algemene uitgangspunt is dan ook dat er te allen tijde in overeenstemming wordt gehandeld met de privacywetgeving. Dit waarborgt een zorgvuldige gegevensverwerking.
Waar de wet ruimte laat voor eigen argumentatie zal de Rechtspraak daar met eigen beleid invulling aan geven. Hierbij is ervoor gekozen dat de hoedanigheid waarin de Rechtspraak handelt en de aard van de gegevens een rol spelen bij de invulling van de ruimte die de privacywetgeving laat. Wanneer de Rechtspraak handelt in de hoedanigheid van rechtsprekende macht en gegevens verwerkt ten behoeve van het primaire proces zullen de open normen in de privacywetgeving strikt geïnterpreteerd worden en zal een hoog ambitieniveau worden nagestreefd. Daarbij is het uitgangspunt: hoe gevoeliger de gegevens, hoe hoger het ambitieniveau. Waar de Rechtspraak opereert als zijnde ieder andere organisatie zullen de open normen – waar mogelijk – minder strikt geïnterpreteerd worden. Ook hierbij geldt: hoe gevoeliger de gegevens, hoe hoger het ambitieniveau

Naast de hoedanigheid waarin de Rechtspraak handelt en de aard van de gegevens, kunnen andere maatschappelijke belangen, zoals openbaarheid richting de maatschappij, en innovatie een rol spelen bij het beleid van de Rechtspraak op het gebied van privacy en de invulling van de open normen.

Wegens de aard van de organisatie, is er binnen de Rechtspraak al veel aandacht voor een zorgvuldige omgang met zaakgegevens van betrokken partijen. Bij de inbedding van de privacywetgeving dient zo veel mogelijk aangesloten te worden bij het reeds bestaande bewustzijn en bestaande processen en procedures, zodat de aankomende privacywetgeving op zo gestructureerde wijze wordt ingebed in de Rechtspraak.

Beleggen rollen en verantwoordelijkheden

Tijdens de sessie zijn tevens een aantal keuzes gemaakt over het beleggen van de verantwoordelijkheden binnen de organisatie. Hierbij is ervoor gekozen om de verantwoordelijkheid voor de ontwikkeling van de normenkaders en richtlijnen met betrekking tot privacy landelijk te beleggen. De voorkeur is uitgesproken om één landelijke FG aan te stellen die een adviserende en informerende rol vervult omtrent de verplichtingen die voortvloeien uit de aankomende privacywetgeving en daarnaast toezicht houdt op de naleving daarvan. De FG zal Raad, gerechten en landelijke diensten van advies gaan voorzien, maar heeft ook de bevoegdheid om Raad, gerechten en landelijke diensten erop te wijzen als er niet in overeenstemming met de wetgeving wordt gehandeld.
Nu er voorafgaand aan de implementatietermijn van de aankomende privacywetgeving nog een aanzienlijk aantal actiepunten en verbeteringen dienen te worden doorgevoerd, wordt het ten zeerste aangeraden om zo spoedig mogelijk op projectbasis een privacyspecialist aan te stellen, dan wel in te huren die het project rondom de implementatie van de aankomende privacywetgeving zal begeleiden en uitvoeren.

Om adequaat uitvoering te geven aan de vereisten van de privacywetgeving, wordt het tevens nodig geacht een privacy officer aan te stellen bij Spir-it en LDCR. Gezien het feit dat het zwaartepunt van de privacyvraagstukken bij Spir-it ligt, wordt het aangeraden de privacy officer bij Spir-it te positioneren en onder verantwoordelijkheid van Spir-it te laten vallen. Naar verwachting zal de privacy officer het merendeel van zijn werkzaamheden bij Spir-it uitvoeren. De privacy officer dient echter ook in staat te worden gesteld om privacyvraagstukken van het LDCR op te vangen. Door aanstelling van een privacy officer wordt in een vroeg stadium aan de 'voorkant' van het proces al veel aandacht besteedt aan de vereisten die voortvloeien uit de privacywetgeving en worden er al veel privacyvraagstukken ondervangen. Waar mogelijk zullen meteen aanpassingen worden doorgevoerd om overeenstemming met de privacywetgeving te bereiken. De rol van de privacy officer dient echter wel los gezien te worden van de rol van de FG. De FG is uitsluitend degene die de wettelijke taken zal verrichten zoals deze in de AVG en de Richtlijn zijn neergelegd. De privacy officer zal verantwoordelijk zijn voor de operationalisering van het beleid binnen Spir-it en, waar nodig LDCR, en zal de normenkaders vertalen naar concrete maatregelen. De privacy officer ondervangt daarnaast de privacyvraagstukken waar medewerkers van Spir-it en LDCR in de uitvoering van hun werkzaamheden tegen aan lopen.

Binnen de gerechten en de landelijke dienst, SSR, zullen de verantwoordelijkheden niet worden herbelegd en zal de wijze waarop privacy thans is ingebed worden voorgezet, wat betekent dat er binnen ieder gerecht en bij het SSR een aanspreekpunt privacy zal zijn.

Actiepunten

Het is van belang dat de verantwoordelijkheden op zo kort mogelijke termijn bij de juiste personen worden belegd. Dit betekent het ten zeerste wordt aangeraden zo spoedig mogelijk op projectbasis een privacyspecialist aan te stellen, dan wel in te huren die het project rondom de implementatie van de aankomende privacywetgeving gaat begeleiden en uitvoeren.
Daarnaast wordt het aanbevolen op termijn – in samenspraak met de huidige FG – te bepalen op welke wijze de rol van de FG uitgebreid zal moeten worden. Voorts dient op korte termijn een privacy officer bij Spir-it aangesteld te worden en op bestuurlijk niveau te worden bepaald op welke wijze de verdeling van de werkzaamheden tussen Spir-it en LDCR concreet vormgegeven gaat worden.
Zodra deze actiepunten zijn doorgevoerd, dan wel een start is gemaakt met deze actiepunten, kunnen de medewerkers die belast zijn met privacy binnen de Rechtspraak spoedig starten met de operationalisering van het plan. Het is aan voornoemde medewerkers om de geformuleerde visie te vertalen naar de door de privacywetgeving gestelde normen, prioritering aan te brengen in de actiepunten zoals genoemd in bijlage I, normenkaders en richtlijnen te ontwikkelen, deze uit te rollen in de organisatie en het bewustzijn te creëren.

1. **Beleggen rollen en verantwoordelijkheden**
    - Er dient een privacyspecialist te worden aangesteld, dan wel te worden ingehuurd die het project rondom de implementatie van de aankomende privacywetgeving gaat begeleiden en uitvoeren.
    - De huidige rol van de FG dient op termijn , in samenspraak met de de huidige FG, uitgebreid te worden, zodat de rol van FG op 25 mei 2018 in overeenstemming is gebracht met de vereisten die voortvloeien uit de privacywetgeving.
    - Er dient een privacy officer aangesteld te worden bij Spir-it. Tevens dient op bestuurlijk niveau te worden bepaald op welke wijze de verdeling van de werkzaamheden tussen Spir-it en LDCR concreet vormgegeven gaat worden.
    - De uitvoerende verantwoordelijkheden voor het implementatietraject dienen duidelijk belegd te worden onder de huidge FG, privacy officer en het privacy team (adviseurs recht en ICT / privacy expertgroep) en mogelijk andere medewerkers die belast zijn met privacy.

2. Opstellen en uitvoeren operationeel plan

- Zodra de verantwoordelijkheden zijn belegd bij de juiste personen, dan wel een start is gemaakt met de herbelegging van de verantwoordelijkheden dienen de medewerkers die met deze verantwoordelijkheid zijn belast zeer spoedig als team samen te komen en te starten met het opstellen van een plan om de genoemde actiepunten in bijlage I aan de hand van de door de Rechtspraak geformuleerde visie door te voeren.

Om ervoor zorg te dragen dat op structurele wijze uitvoering wordt gegeven aan de privacywetgeving binnen de Rechtspraak, wordt het aangeraden om de privacy strategie na enige tijd te evalueren en waar nodig aan te passen naar eventuele veranderingen in wetgeving, maatschappelijke veranderingen en veranderende behoeftes binnen de organisatie.

Bijlage I – schematische weergave concrete actiepunten

Strategisch privacy plan

Operationeel privacy plan

Documenteren gegevensverwerkingen
• In kaart brengen IT gegevensverwerkingen[27]
• De medewerkers die belast zijn met privacy binnen de Rechtspraak brengen overige gegevensverwerkingen in kaart
• De medewerkers die belast zijn met privacy binnen de Rechtspraak leggen gegevensverwerkingen vast in documentatiemap
• De medewerkers die belast zijn met privacy binnen de Rechtspraak beoordelen of gegevensverwerkingen zijn toegestaan
• Aldoor blijven aanpassen van documentatiemap naar eventuele nieuwe gegevensverwerkingen

Aanpassen processen en procedures
• Contracten, waaronder bewerkersovereenkomsten, in overeenstemming brengen met privacywetgeving
• Aanpassen proces omtrent het uitvoeren van privacy impact assessments en integreren privacy by design en default
• Updaten extern privacy beleid website + ontwikkelen extern privacy beleid voor de KEI systemen
• Opstellen intern privacy beleid
• Herijken procedures datakwaliteit en bewaartermijnen
• Herijken inrichting Datalekteam
• Procedures vaststellen rechten betrokkenen
• Blijf beleid en procedures omtrent fysieke en informatiebeveiliging evalueren en pas waar nodig aan

Cultuur en bewustwording
• Bewustwordingscampagne privacy
• Trainingen, workshops en educatie voor medewerkers
• Bied – waar mogelijk- hulpmiddelen aan (FAQ's e.d.)

Monitoring en handhaving
• Handhaaf bij non-compliance
• Lessons learned
• Pas het privacy beleid aan

[27] Op dit moment loopt er een vooronderzoek naar het in kaart brengen van de gegevensverwerkingen. Het vooronderzoek wordt uitgevoerd door medewerkers van Spir-it en LDCR, in samenwerking met medewerkers van de Raad.

Deelbesluit 1 - Datalekken
Document 3

Privacy Governance Rechtspraak

Doelstelling
Met dit kader worden de verantwoordelijkheden in relatie tot de verwerking van persoonsgegevens binnen de Rechtspraak vastgesteld.

Definities
De definities van veel voorkomende begrippen staan beschreven in de AVG en de Richtlijn. Een overzicht van veel voorkomende definities wordt gegeven in het '*Definitiekader AVG en Richtlijn*'.

Wie is verantwoordelijk?
Verantwoordelijken voor de verwerking van persoonsgegevens zijn volgens de AVG en de Richtlijn diegenen die het doel en de middelen van verwerking bepalen. Voor de Rechtspraak betekent dit dat de verwerking van persoonsgegevens gebeurt onder verantwoordelijkheid van:

- De besturen van rechtbanken, gerechtshoven en bijzondere appelcolleges (CRvB, CBb);
- De Raad voor de rechtspraak (mede als eigenaar van de landelijk diensten).

Aangezien de Raad en de gerechten vaak gezamenlijk de doelen en middelen van verwerking bepalen, is er in veel gevallen sprake van een 'gezamenlijke verantwoordelijkheid'. Op basis van de AVG en de Richtlijn zijn zij dan verplicht 'op transparante wijze de respectievelijke verantwoordelijkheden vast te stellen'.

Hoe is die verantwoordelijkheid verdeeld?

- De Raad voor de rechtspraak is verantwoordelijk voor ondersteuning, financiering en toezicht ten aanzien van de bedrijfsvoering van gerechten, ook voor wat betreft de toepassing en naleving van de AVG en de Richtlijn. Dit vloeit voort uit artikel 91 van de Wet op de rechtelijke organisatie.
- Als eigenaar van de landelijke diensten stelt de Raad in overleg met gerechten en diensten doel en middelen van de gegevensverwerkingen in landelijke IT applicaties en diensten vast. De Raad is eindverantwoordelijk voor de borging dat landelijke IT applicaties en diensten zijn ingericht conform de beginselen van de AVG en de Richtlijn.
- De directeuren van de landelijke diensten en de bestuurder van SSR[1] zijn namens de Raad voor de rechtspraak verantwoordelijk voor de borging en leggen hierover verantwoording af aan de Raad.
- Het bestuur van elk gerecht stelt doel en middelen voor verwerking van persoonsgegevens vast. Het gerechtsbestuur is daarmee eindverantwoordelijk voor de toepassing en naleving van de AVG en de Richtlijn door medewerkers van dat gerecht. Daaronder valt ook het verlenen van toegang tot persoonsgegevens waaronder het lokale autorisatiebeheer van landelijke IT-applicaties.
- Het gerechtsbestuur is ook eindverantwoordelijk voor de verwerking van persoonsgegevens in lokale IT-applicaties of dienstverlening die zelf zijn aangekocht, bijvoorbeeld bij derden.

Ontwikkeling en aanpassing van (nieuwe) processen en systemen
De Raad voor de rechtspraak ontwikkelt in samenspraak met de gerechten processen en systemen. Om ervoor te zorgen dat de AVG en de Richtlijn worden nageleefd, maken Raad en gerechten heldere afspraken over de voorwaarden waaronder de ontwikkeling en aanpassing plaatsvindt. De volgende regels zijn daarvoor van toepassing:

- Opdrachtgevers binnen de Rechtspraak die belast zijn met de ontwikkeling of aanpassing van processen en systemen zijn verplicht te zorgen dat alle processen en systemen conform de AVG en de Richtlijn zijn ingericht (privacy door ontwerp) en dat dit kan worden aangetoond.
- Voor nieuwe processen of systemen of aanpassingen met gevolgen voor de verwerking van persoonsgegevens dient een (verkorte of volledige) Privacy Impact Assessment (PIA) te worden

[1] De Privacy Governance van SSR wordt nader uitgewerkt in afspraken tussen het College van Bestuur en de Raad van Eigenaren van SSR.

uitgevoerd. De opdrachtgever is verplicht de PIA ter toetsing voor te leggen aan de Functionaris Gegevensbescherming.
- Onderdeel van de acceptatiecriteria van nieuwe IT-applicaties of dienstverlening is de aanwezigheid van een PIA en of de privacy maatregelen zoals ontworpen, zijn doorgevoerd. Daarbij worden afspraken gemaakt over de uitvoering van het beheer en het doorvoeren van aanpassingen na implementatie.
- Bij ontwikkelingen met een grote impact of als er sprake is van fundamenteel verschil van inzicht over de verwerking van persoonsgegevens vindt besluitvorming in overeenstemming met de besluitvormingsprocedures zoals deze gelden in de governance structuur van de Rechtspraak. Daarbij wordt altijd eerst de functionaris gegevensbescherming geconsulteerd.

Verwerkers

'Verwerkers' zijn externe leveranciers of dienstverleners die in opdracht van de Rechtspraak persoonsgegevens verwerken. Wie deze leveranciers of dienstverleners zijn, blijft hier buiten beschouwing. De Rechtspraak blijft echter eindverantwoordelijk. De AVG en de Richtlijn schrijven voor dat met deze externe partijen een verwerkersovereenkomst wordt afgesloten. Hoe dit proces precies verloopt, staat beschreven in de *Procedure verwerkersovereenkomsten*. Daarin staat ook wanneer wel of wanneer geen overeenkomst nodig is. Tussen overheden onderling bijvoorbeeld is het afsluiten van een verwerkersovereenkomst niet nodig, maar wel dient dan een 'verwerkersprotocol' te worden opgesteld.

Verdeling van rollen en taken

Raad voor de rechtspraak

De Raad voor de rechtspraak wijst één van zijn leden als portefeuillehouder privacy aan. De FG en de beleidsadviseur privacy adviseren en ondersteunen de portefeuillehouder privacy. De taken en rollen die daarbij horen zijn terug te vinden in *bijlage A*.

Rechtbanken en hoven

Ieder gerechtsbestuur wijst uit haar midden een portefeuillehouder privacy aan. De coördinator privacy in het gerecht (meestal de beveiligingscoördinator of een functionaris die nauw samenwerkt met de beveiligingscoördinator) en een coördinator informatieverzoeken (meestal de bestuurssecretaris of klachtenfunctionaris) ondersteunen de portefeuillehouder. Dit kan ook een privacy team zijn met verdeling van de taken over meerdere functionarissen. De taken en rollen binnen de gerechten zijn nader omschreven in *bijlage B*.

Landelijke diensten

De directeuren van de landelijke diensten en de bestuurder van SSR zijn namens de Raad verantwoordelijk voor de verwerkingen van persoonsgegevens in hun dienst. Er is een Privacy Officer aangesteld bij IVO die verantwoordelijk is voor de toepassing en naleving van de AVG in de centrale IT- applicaties en daaraan gerelateerde dienstverlening. Bij SSR en LDCR is een privacy coördinator aangewezen om het privacybeleid binnen die diensten verder te verbeteren. De taken en rollen binnen de landelijke diensten zijn nader omschreven in *bijlage C*.

In *bijlage D* wordt voorts een nadere toelichting gegeven op de verdeling van taken op een aantal beleidsonderdelen.

Uitvoeringsverantwoordelijkheden afdelingen en teams

De FG, de Privacy Officer IVO, de lokale privacy coördinatoren en de coördinatoren informatieverzoeken hebben een coördinerende en adviserende rol in de uitvoering van het privacy beleid. De verantwoordelijkheid voor de uitvoering ligt echter bij de leidinggevenden en medewerkers van afdelingen en teams die de dagelijkse verantwoordelijkheid dragen voor het verwerken van persoonsgegevens.
Hiervoor gelden de volgende aanbevelingen:

- Stel de leidinggevenden op de hoogte dat zij verantwoordelijk zijn voor de verwerking van persoonsgegevens door hun afdeling of team en informeer hen over het privacybeleid;
- Zorg dat binnen iedere afdeling of team een medewerker is aangewezen als aanspreekpunt voor de interne privacyfunctionarissen en die als 'privacy champion' binnen het team kan fungeren. Deze medewerker is ook aanspreekpunt mochten er incidenten plaatsvinden die samenhangen met verwerking van persoonsgegevens door de afdeling of het team.
- Informeer alle medewerker over hun eigen verantwoordelijkheid om ervoor te zorgen dat persoonsgegevens op rechtmatige, behoorlijke en transparante wijze worden verwerkt en dat zij voor vragen terecht kunnen bij de interne privacyfunctionarissen.

Afhankelijk van het werkgebied is er sprake van wisselende verantwoordelijkheid. Zo is Inkoop verantwoordelijk voor het afsluiten van verwerkersovereenkomsten met externe leveranciers en de beveiligingscoördinator verantwoordelijk voor het beveiligingsbeleid. In *bijlage E* staat een overzicht van de verschillende uitvoeringsverantwoordelijkheden.

Intern toezicht, extern toezicht en rechtsbescherming

Volgens de AVG en de Richtlijn zijn verwerkingsverantwoordelijken verplicht mee te werken aan onafhankelijk intern en extern toezicht op de toepassing en naleving van de AVG en de Richtlijn.
De FG is, zoals eerder beschreven, belast met het interne toezicht op de verwerking van persoonsgegevens door gerechten en diensten. De FG is werkzaam bij het bureau Raad en adviseert en ondersteunt de portefeuillehouder privacy van de Raad voor de rechtspraak.
In de AVG (hoofdstuk VI en VII) en de Richtlijn is de inrichting van het externe toezicht en de rechtsbescherming beschreven. Voor de Rechtspraak geldt vanwege haar onafhankelijk positie in het staatsbestel een bijzondere situatie. De uitwerking van het extern toezicht en de rechtsbescherming wordt daarom beschreven in een aparte regeling.

Vaststelling privacy governance

Dit beleidskader is vastgesteld door de Raad voor de rechtspraak en de Presidentenvergadering op mandaat van de gerechtsbesturen op 14 mei 2018.

Bijlage A: Taken functionaris gegevensbescherming en beleidsadviseur privacy

Taken functionaris gegevensbescherming

De Functionaris gegevensbescherming (FG) heeft conform de AVG, de Richtlijn en de 'regeling toezicht verwerking persoonsgegevens Rechtspraak' (Hoge Raad, versie 17 april 2018) de volgende taken:

a) de Raad, gerechten en het parket bij de Hoge Raad informeren en adviseren over hun verplichtingen uit hoofde van de Algemene Verordening Gegevensbescherming (verder: AVG) en de krachtens de Richtlijn EU 2016/680, L 119/89 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (verder: de Richtlijn) vastgestelde bepalingen;
b) toezien op naleving van de AVG en de krachtens de Richtlijn vastgestelde bepalingen en van het beleid door de Raad en de gerechten met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel;
c) desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling (Privacy Impact Assessments) en toezien op de uitvoering daarvan in overeenstemming met artikel 35 AVG;
d) desgevraagd advies verstrekken met betrekking tot datalekken;
e) desgevraagd advies verstrekken met betrekking tot de procedure rechten van betrokkenen;
f) met de PGHR samenwerken;
g) optreden als contactpunt voor de PGHR inzake met verwerking verband houdende aangelegenheden;
h) optreden als contactpunt voor de Autoriteit persoonsgegevens inzake met verwerking verband houdende aangelegenheden.

De FG werkt bij de uitoefening van taken nauw samen met de landelijk beveiligingsambtenaar, de beleidsadviseur privacy bij de Raad en de Privacy Officer bij IVO. De FG fungeert als aanspreekpunt en adviseur voor privacyfunctionarissen bij gerechten en diensten. De FG is ook verantwoordelijk voor de communicatie, afstemming en samenwerking met externe belanghebbenden en ketenpartijen ten aanzien van de verwerking en uitwisseling van persoonsgegevens. De FG legt jaarlijks verantwoording af aan de Raad voor de rechtspraak over de uitvoering van werkzaamheden door de FG.

Taken beleidsadviseur privacy

De beleidsadviseur privacy is belast met de volgende taken:

a) ontwikkelen en borgen van landelijk privacybeleid en daaruit voortvloeiende procedures en richtlijnen;
b) ontwikkelen van landelijk beleid over PDCA, administratieve organisatie en interne controle;
c) bevorderen van landelijke bewustwording en educatie;
d) coördineren van het beheer en de actualisatie van het landelijk register van verwerkingen;
e) coördineren van de landelijke afstemming in verband met de procedure datalekken;
f) coördineren van de landelijke afstemming in verband met de procedure rechten betrokkenen. In dat kader fungeert de beleidsadviseur privacy tevens als de 'landelijk coördinator informatieverzoeken'. Voor meer informatie wordt verwezen naar de 'procedure rechten betrokkenen';
g) Eerste aanspreekpunt beantwoording van interne en externe vragen op het terrein van de AVG en de Richtlijn;
h) Overige taken (nader in te vullen).

Eventuele benodigde extra capaciteit voor de vervulling van de rol van FG en beleidsadviseur privacy zal de komende maanden op basis van ervaring en een evaluatie nader worden bepaald en worden terug gekoppeld aan de Raad voor de rechtspraak en het PRO.

Bijlage B: Taken privacy coördinatoren en coördinatoren informatieverzoeken gerechten

Privacy coördinatoren gerechten

De privacy coördinatoren van gerechten zijn belast met de volgende taken:

a) vertalen en operationaliseren van landelijk privacybeleid naar lokale processen;
b) coördinatie van de PDCA-cyclus, administratieve organisatie en de interne controle;
c) bevorderen van lokale bewustwording en educatie;
d) beheer lokale deel register van verwerkingen (lokale IT applicaties en lijsten met persoonsgegevens);
e) uitvoering administratieve organisatie en interne controle;
f) uitvoeren privacy impact assessments voor specifieke lokale processen en systemen;
g) uitvoeren procedure melden van datalekken;
h) uitvoering procedure rechten betrokkenen;
i) overige taken (nader in te vullen).

De rol van privacy coördinator wordt toebedeeld aan één functionaris. De taken van de privacy coördinator kunnen eventueel gedelegeerd worden aan andere functionarissen. De tijdsbesteding voor het vervullen van deze rol is afhankelijk van de omvang van het gerecht en de intensiteit waarmee het gerecht invulling wil geven aan deze rol. Vooral in het eerste jaar na implementatie zal meer gevraagd worden van de privacy coördinator om het privacybeleid structureel in te bedden in de organisatie. De gerechten wordt geadviseerd in het eerste jaar meer aandacht te besteden aan deze functie onder meer door het bieden van extra ondersteuning.

Coördinatoren informatieverzoeken gerechten

De coördinator informatieverzoeken is belast met de volgende taken:

a) het informeren van betrokkenen en het behandelen verzoeken van betrokkenen volgens vastgestelde procedures;
b) het afhandelen van verzoeken in overleg met uitvoeringsverantwoordelijken in afdelingen of teams;
c) het afstemmen van verzoeken van betrokkenen in de strafrechtketen met het Openbaar Ministerie en/of het eventueel doorverwijzen van verzoeken naar het Openbaar Ministerie;
d) de afhandeling van klachten over verwerking van persoonsgegevens namens het gerechtsbestuur;
e) samenwerken met de beleidsadviseur privacy (tevens landelijk coördinator informatieverzoeken) en de FG bij afhandeling van klachten en verzoeken;
f) het informeren van betrokkenen over vervolgstappen indien zij ontevreden zijn over de afhandeling van een verzoek of klacht;
g) overige taken (nader in te vullen)**.**

De rol van coördinator informatieverzoeken kan logischer wijs het beste belegd worden bij de klachtenfunctionaris of bestuurssecretaris. Dit omdat klachten over verwerkingen van persoonsgegevens doorgaans ook door worden afgehandeld. De tijdsbesteding die daarmee gemoeid is hangt af van het aantal verzoeken dat jaarlijks binnenkomt. Onder de Wet bescherming persoonsgegevens was het aantal verzoeken beperkt. Mogelijk neemt dit aantal onder de AVG toe, vooral de eerste maanden na implementatie door de toegenomen publieke aandacht voor privacy. Vooralsnog is de inschatting dat de voor de afhandeling van deze verzoeken geen extra ondersteuning nodig is. Ook omdat het bureau Raad de eerste maanden na implementatie extra ondersteuning biedt.

Eventuele benodigde extra capaciteit voor de vervulling van de rol van privacy coördinator en de coördinator informatieverzoeken zal in de komende maanden op basis van ervaring en een evaluatie worden bepaald en worden gedeeld met de Raad voor de rechtspraak en het PRO

Bijlage C: Taken Privacy Officer IVO en privacy coördinatoren landelijke diensten

Privacy Officer IVO

De Privacy Officer van IVO is primair belast met het borgen van de naleving van de AVG en de Richtlijn met betrekking tot de door IVO beheerde centrale IT-applicaties. Omdat de andere landelijke diensten (LDCR, SSR en bureau Raad) gebruik maken van IT-applicaties van IVO voor verlening van diensten, fungeert de Privacy Officer IVO tevens als adviseur en ondersteuner voor de privacy coördinatoren van de landelijke diensten.
De functie van Privacy Officer is een fulltime functie. De exacte invulling van de taken van de Privacy Officer IVO wordt in nader overleg met de directie van IVO bepaald.

Privacy coördinatoren landelijke diensten

De privacy coördinatoren van landelijke diensten zijn verantwoordelijk voor het bevorderen van de naleving van de AVG en de Richtlijn voor de lokale processen en voor de landelijke dienstverlening aan gerechten en andere landelijke diensten. De privacy coördinatoren van de landelijke diensten werken nauw samen met de Privacy Officer van IVO aangezien een belangrijk deel van de diensten wordt verleend met behulp van centrale IT-applicaties. De tijdsbesteding voor de privacy coördinatoren van de landelijke diensten hangt van de omvang van de organisatie af en of de dienstverlening meer of minder tijd kost.
De precieze invulling van de taken van de privacy coördinatoren worden in overleg met de directies van de landelijke diensten en het bestuur van SSR bepaald. De komende maanden worden de Raad voor de rechtspraak en het PRO daarover geïnformeerd.

Bijlage D: Verdeling taken Raad, gerechten en diensten per beleidsonderdeel
Hieronder geven we aan de hand van een aantal beleidsonderdelen verduidelijking over de verdeling van de verantwoordelijkheden tussen Raad, gerechten en diensten Het gaat niet om een compleet overzicht van taken. Meer informatie daarover is te lezen in *'Privacybeleid Rechtspraak'*.

Privacybeleid
De Raad voor de rechtspraak is verantwoordelijk voor het ontwikkelen van een landelijk uniform en door de gerechten en diensten gedragen privacybeleid en daaruit voortvloeiende handreikingen en procedures.
Het privacybeleid komt tot stand op basis van dialoog en samenwerking met de gerechten en diensten.
Indien wenselijk en nodig kan door oprichting van landelijke overleggen en werkgroepen op deelonderwerpen het privacybeleid en overige privacyvraagstukken verder worden geoptimaliseerd en geprofessionaliseerd. De gerechten en diensten zijn verantwoordelijk voor vertalen en operationaliseren van het gezamenlijk ontwikkelde privacybeleid naar lokaal privacybeleid. Voor meer informatie, zie: '*Privacybeleid Rechtspraak'.*

Bewustwording en educatie
De Raad voor de rechtspraak is verantwoordelijk voor het landelijk beleid om de bewustwording en educatie over privacy te bevorderen. De Raad zorgt voor een interne communicatiestructuur met een Landelijke Intropagina over privacy, wiki-pagina's en kennisdeling via MKO. Presentaties en factsheets helpen de kennis en educatie over privacy te bevorderen evenals opleidingen en cursussen. Hierbij wordt samengewerkt met SSR en LDCR. Tot slot zal via nieuwsberichten op Intro Landelijk en bijvoorbeeld een postercampagne regelmatig aandacht worden gevraagd voor privacy. De gerechten en diensten krijgen handvatten mee om op lokaal niveau de bewustwording en educatie te bevorderen en zijn verantwoordelijk voor de lokale uitrol.
Voor meer informatie, zie: '*beleidskader privacy interne bewustwording en educatie'.*

Verzoeken en klachten van betrokkenen en andere belanghebbenden
Verzoeken van betrokkenen en andere belanghebbenden kunnen op verschillende manieren binnen komen[2].
Bij een gerecht zelf, bij de Raad voor de rechtspraak of via het RSC. De coördinator informatieverzoeken van het gerecht (meestal een bestuurssecretaris of klachtenfunctionaris) is primair verantwoordelijk voor het afhandelen van verzoeken en klachten van betrokkenen. De coördinator informatieverzoeken kan advies vragen aan de landelijk coördinator informatieverzoeken. Indien een verzoek betrekking heeft op meerdere gerechten, complex of gerecht overstijgend is, coördineert de landelijke coördinator informatieverzoeken de afhandeling. Als betrokkenen een klacht hebben over de wijze van afhandeling dan draagt de coördinator zorg voor de verdere afhandeling van de procedure en de eventuele doorverwijzing naar beroepsinstanties. Alle verzoeken en klachten van betrokkenen en de wijze van afhandelen worden geregistreerd in een register. Voor meer informatie, zie: '*interne procedure rechten betrokkenen'*.

Administratieve organisatie en interne controle
De Raad voor de rechtspraak houdt toezicht op de toepassing en naleving van de AVG en de Richtlijn door de gerechten en de diensten en ontwikkelt een landelijk beleid voor administratieve organisatie en interne controle. Gerechten en diensten vertalen dit beleid naar de lokale situatie. De accountant controleert op basis van de AO/IC van gerechten en diensten opzet, bestaan en werking van het privacybeleid. Voor meer informatie zie: '*beleidskader privacy administratieve organisatie en interne controle*'.

Privacy Impact Assessments en Privacy by Design
De Raad voor de rechtspraak is verantwoordelijk voor de landelijke coördinatie van Privacy Impact Assessments (PIA's). Bij de ontwikkeling van een nieuw IT-systeem is IVO verantwoordelijk voor de coördinatie van de uitvoering van de PIA. Dat geldt ook voor nieuwe producten van LDCR, SSR, en het bureau Raad. De PIA moet altijd goedgekeurd worden door de opdrachtgever voor een nieuw proces, systeem of dienst (proceseigenaar).

[2] Voor de eenvoud wordt hier alleen ingegaan op de procedure als een betrokkene een verzoek indient bij een gerecht.

Voorts wordt de PIA altijd ter goedkeuring voorgelegd aan de FG. Voor meer informatie, zie: '*procedure privacy impact assessment'* en '*beleidskader door ontwerp en standaardinstellingen'*.

Register van verwerkingen

De Raad voor de rechtspraak is verantwoordelijk voor het houden van één landelijk register van verwerkingen voor de Rechtspraak en draagt er zorg voor dat het landelijk register regelmatig wordt geactualiseerd.
De landelijke diensten zijn in dat kader verantwoordelijk voor het deel van het register van verwerking dat betrekking heeft op centrale IT applicaties (IVO) en landelijke dienstverlening waarbij persoonsgegevens worden verwerkt (LDCR, SSR, bureau Raad). De gerechten zijn verantwoordelijk voor het bijhouden van het lokale deel van het landelijke register van verwerkingen (bijvoorbeeld het register van lijsten met persoonsgegevens). Voor meer informatie, zie: '*procedure verwerkingsregister Rechtspraak*'.

Datalekken

Als er sprake is van een datalek (onrechtmatige inzage, verlies en diefstal) dan treedt de meldprocedure datalekken in werking waarbij binnen 72 uur de nodige acties uitgezet moeten worden om het datalek op de juiste manier af te handelen. Op lokaal niveau zijn beveiligingscoördinatoren en privacy coördinatoren verantwoordelijk voor de afhandeling van het datalek. Bij de Raad voor de rechtspraak is een datalekteam aanwezig dat verantwoordelijk is voor de landelijke coördinatie van deze procedure. Alle datalekken worden op lokaal niveau geregistreerd in een register. Voor meer informatie, zie: *'procedure datalekken'*.

Bijlage E: Overzicht van uitvoeringsverantwoordelijkheden

De hoofden van afdelingen en teams zijn uitvoeringsverantwoordelijk voor naleving van de AVG en de Richtlijn. Afhankelijk van het werkgebied, kan onderscheid gemaakt worden tussen de volgende typen uitvoeringsverantwoordelijkheden:

- Informatietechnologie (ICT): uitvoeringsverantwoordelijk voor de inrichting van datamodellen in IT systemen en het doorvoeren van privacy maatregelen in IT systemen waaronder het bewaren en verwijderen van data in systemen;
- Integrale beveiliging: uitvoeringsverantwoordelijk voor passende beveiliging van persoonsgegevens;
- Functioneel beheer: uitvoeringsverantwoordelijk voor het doorvoeren van aanpassingen in IT applicaties met persoonsgegevens en het autorisatiebeheer;
- HRM / P&O: uitvoeringsverantwoordelijk voor privacy maatregelen met betrekking tot sollicitanten, medewerkers en voormalig medewerkers;
- Financiën: verantwoordelijk voor de uitvoering van privacy maatregelen met betrekking tot financiële gegevens over debiteuren en crediteuren;
- Inkoop: uitvoeringsverantwoordelijk voor het afsluiten van verwerkersafspraken met externe leveranciers en dienstverleners;
- Archief: uitvoeringsverantwoordelijk voor het archiefbeleid met betrekking tot persoonsgegevens;
- Communicatie: uitvoeringsverantwoordelijk voor interne en externe communicatie waaronder het delen van informatie met de pers, maatschappelijke actoren en de samenleving;
- Facilitair: uitvoeringsverantwoordelijk voor de verwerking van persoonsgegevens in het kader van de facilitaire dienstverlening waaronder het verwerken van persoonsgegevens voor inwonende partijen;
- Planning en control: uitvoeringsverantwoordelijk voor de interne controle op de administratieve organisatie met betrekking tot privacy management;
- Overige uitvoeringsverantwoordelijkheden (nader in te vullen).

Deelbesluit 1 - Datalekken
Document 4

(4E) Borgingsplan Privacy Rechtspraak

Versie 26 maart 2020

Inleiding

Met dit borgingsplan worden de activiteiten van de Rechtspraak t.a.v. privacy inzichtelijk gemaakt. Met de activiteiten in dit plan wordt beoogd om niet alleen te voldoen aan de verplichtingen van de Algemene Verordening Gegevensbescherming(AVG), maar ook aan de verplichtingen die voortvloeien uit de Wet Strafvorderlijke en Justitiële Gegevens(WSJG). Daarbij is het niet alleen van belang dat op een bepaald moment aan de eisen wordt voldaan, maar dat dit ook structureel is geborgd. Bij toekomstige ontwikkelingen binnen de Rechtspraak dient ook aandacht besteed te worden aan privacy.

Dit plan is ingedeeld conform de indeling van de J&V-indicatoren voor de implementatie van de AVG. Daarnaast is er een categorie overig. In de tekst wordt telkens aangegeven welke scores er worden gehanteerd en waar de Rechtspraak staat. Vervolgens wordt aangegeven welke activiteiten de rechtspraak t.a.v. de betreffende indicator onderneemt en vervolgens wordt afgesloten met een indicatorscore waar de Rechtspraak staat.

De werkwijze die bij dit borgingsplan gehanteerd wordt, is dat er sprake is van een plan dat minimaal halfjaarlijks wordt herijkt. Het 1e borgingsplan is door de Raad voor de rechtspraak in januari 2019 vastgesteld. Het 2e borgingsplan bevatte de stand van zaken per 1 mei 2019. Het 3e borgingsplan bevatte de stand van zaken per 1 november 2019. Dit 4e borgingsplan bevat de stand van zaken per 1 maart 2020. Voor de werkzaamheden bij IVO is aan dit borgingsplan een gedetailleerde roadmap gekoppeld.

Dit plan gaat niet in op de activiteiten die door het Landelijk Bureau Vakinhoud rechtspraak (LBVr) worden verricht, waarbij het gaat om de werkzaamheden die liggen in het verlengde van het werk van de rechter. Binnen het LBVr is er een jurist die vakinhoudelijke vragen t.a.v. de AVG coördineert en die secretaris is van de werkgroep AVG vakinhoud. De werkgroep AVG vakinhoud is op verzoek van de LOV's opgericht en bestaat uit experts vanuit de gerechten. De leden beschikken over specifieke vakinhoudelijke AVG-kennis. Ook is er een Wikipagina AVG voor het primaire proces van de rechtspraak, waarin (Europese) jurisprudentie e.d. wordt bijgehouden. Hierop zijn ook de antwoorden op de vakinhoudelijke vragen en een overzicht van veel gestelde vragen raadpleegbaar zijn. Vanzelfsprekend is er wel samenwerking en uitwisseling van kennis tussen LBVr en de betrokkenen vanuit de bedrijfsvoering van de Rechtspraak.

AVG overall beeld: in-control

De score werkt als volgt. Het onderdeel is in-control ten aanzien van de implementatie van de AVG. Een onderdeel is in control als het verantwoordelijk management van het onderdeel inzicht heeft in de huidige stand van zaken over de implementatie van de AVG en de risico's met betrekking tot verzamelingen van persoonsgegevens, beschikt over een plan om de AVG te implementeren, de benodigde resources beschikbaar zijn en dat de voortgang periodiek wordt gemonitord. Tevens moet een FG benoemd zijn. Indien eraan wordt gewerkt om in control te komen, dan scoort een onderdeel oranje. Als geen plan voorhanden is en er wordt niet aan gewerkt om op korte termijn alsnog een plan op te leveren, dan scoort een onderdeel rood.

AVG-compliance: voldoet volledig aan de AVG
Het onderdeel heeft de AVG verplichtingen geïmplementeerd in de organisatie. Deze vraag is letterlijk gesteld aan elk onderdeel. Niet compliant en geen plan leidt tot rood, niet compliant maar wel een plan leidt tot een oranje score.

Overall-aanpak
Dit borgingsplan is opgesteld in opdracht van de Raad voor de rechtspraak. Opdrachtnemer is de directeur van het Bureau van de Raad voor de rechtspraak.

De uitvoering van de activiteiten wordt gecoördineerd door een werkgroep met daarin de volgende deelnemers:

- Functionaris gegevensbescherming
- Privacy officer IVO
- Teamleider security, privacy & kwaliteit IVO, tevens wnd CISO
- Hoofd CIO Office
- Beleidsmedewerker privacy bureau Rvdr
- (senior)adviseurs Recht & ICT afdeling Strategie Bureau Rvdr

Agendalid: stafmedewerker Europees recht Landelijk Bureau Vakinhoud rechtspraak

De daadwerkelijke uitvoering van de activiteiten ligt bij een veel grotere groep medewerkers waarbij medewerkers op het terrein van informatiebeveiliging, service delivery, architectuur, applicatie beheer, inkoop, portefeuillehouders en de lokale privacy coördinatoren bij de gerechten belangrijke partijen zijn.

Rechtspraakscore:
Met dit borgingsplan heeft het management inzicht in de stand van zaken van de implementatie van de AVG. De score is daarmee groen op het gebied van in-control en oranje op compliance.

1. AVG-compliance: FG benoemd

De Functionaris Gegevensbescherming is verplicht voor een publieke organisatie; deze geeft advies binnen de organisatie en moet toezien op de juiste uitvoering van de AVG binnen een organisatie. De functie en de taken van deze functie zijn specifiek beschreven in de verordening. De KPI ziet toe op het feit of de FG is benoemd dan wel is aangewezen in een ander organisatieonderdeel om taken uit te voeren. Een onderdeel scoort groen als een FG benoemd is. Een onderdeel scoort rood als geen FG is benoemd. De score oranje wordt niet gebruikt bij deze KPI.

1.1 Evaluatie privacy functies

Een jaar na inwerkingtreding van de AVG is er een evaluatie uitgevoerd door de directeur van het Bureau van de Raad omtrent de benodigde capaciteit waarin specifiek ook aandacht wordt gegeven aan de capaciteit van de functionaris gegevensbescherming. Op basis van de evaluatie is besloten om een functie beleidsadviseur privacybeleid/informatiebeveiliging gerechten bij het bureau BVA te creëren. Deze functie is per 1 oktober 2019 daadwerkelijk ingevuld. Ook is besloten door de Raad voor de rechtspraak om de taken van de Chief Information Security Officer over te hevelen naar IVO. Voorts is bij IVO het aantal fte's qua privacy met 1 fte uitgebreid naar 3 fte.

De huidige inrichting van het toezicht en de verdeling van rollen en verantwoordelijkheden tussen Raad, gerechten en diensten ten aanzien van de AVG en de Wjsg was vastgelegd in twee documenten welke door de Raad en het PRO (met mandaat van de gerechtsbesturen) op 14 mei 2018 zijn vastgesteld (privacybeleid en privacygovernance). Deze documenten zijn geactualiseerd en in september 2019 door MT bureau Rvdr en de BVA vastgesteld. De documenten maken formeel onderdeel uit van het Handboek Integrale Beveiliging, waarvan de formele actualisatie in het SBO maart 2020 wordt afgerond.

1.2 Aanstellen plv. functionaris gegevensbescherming

De ervaring heeft laten zien dat de privacy borging kwetsbaar is als er geen plaatsvervanger is aangesteld voor de FG. Er zijn daarom twee plaatsvervangende functionarissen gegevensbescherming aangesteld. Er is voor gekozen voor dat de privacy officer van IVO die toezichthoudende taken voor de gerechten en het Bureau van de Raad overneemt en de beleidsmedewerker privacy Rvdr de toezichthoudende taak vervangt omtrent zaken van IVO. De betreffende werkwijze is met ingang van 1 oktober daadwerkelijk in werking getreden.

Met het vertrek van de functionaris gegevensbescherming is tijdelijk een waarnemend functionaris gegevensbescherming aangesteld. Per 1 april 2020 treedt de nieuwe functionaris gegevensbescherming aan.

<u>Rechtspraakscore</u>

Er is op dit moment een waarnemend functionaris gegevensbescherming benoemd. Per 1 april treedt de nieuwe, functionaris gegevensbescherming aan en is de Rechtspraak weer op volle sterkte. De achtervang blijft hetzelfde. De score is daarmee: groen.

2. Rechtmatigheid verwerking

Oorspronkelijk lag de focus bij deze KPI op rechtmatigheid van de verwerking van de bijzondere categorieën persoonsgegevens. Ondertussen is dit uitgebreid naar de rechtmatigheid van verwerking van alle persoonsgegevens. Hiermee wordt bedoeld dat een grondslag aanwezig is voor de rechtmatige verwerking. Indien nog niet duidelijk is of één en ander rechtmatig wordt verwerkt maar wel een plan aanwezig is om dit geregeld te krijgen, wordt oranje gescoord. Geen plan met daarin een duidelijke einddatum leidt tot een rode score.

2.1 Verantwoordelijkheid rechtmatige verwerking

Binnen de Rechtspraak zijn de gerechten en diensten zelf verantwoordelijk voor compliance aan de AVG en de Richtlijn. De privacy coördinator is binnen het gerecht het aanspreekpunt op het gebied van privacy. Door de projectleiding van het AVG project van de Rvdr zijn de lokale privacy coördinatoren in vijf themabijeenkomsten bewust gemaakt van de grondslagen en beginselen van de AVG. Indien er verwerkingen zijn die mogelijk onrechtmatig, onbehoorlijk of onvoldoende transparant zijn, behoren die gemeld te worden aan de FG. De FG kent binnen de gehele rechtspraak een adviesrecht.

2.2 Landelijk overleg privacy coördinatoren

De verantwoordelijkheid voor het privacy beleid ligt bij de privacy coördinatoren van gerechten en landelijke diensten. Uit de beveiligingsbenchmark gerechten 2019 d.d. 29 juli 2019 blijkt dat achttien van de twintig organisaties beschikken over een privacy team waarop een beroep gedaan kan worden om te beoordelen of er sprake is van een vermeldenswaardig datalek. Alleen Hof Amsterdam en Hof ‘s-Hertogenbosch beschikken niet over een privacy team. Per 1 maart 2020 is de status hiervan ongewijzigd.

In maart en juni 2019 hebben er bijeenkomsten plaatsgevonden voor de betrokkenen bij privacy bij de rechtspraak. Themagewijs zijn daar onderwerpen besproken. Het structurele karakter van de overleggen was hiermee echter nog niet geborgd. Vanaf 1 oktober maakt het organiseren van dergelijke bijeenkomsten deel uit van het takenpakket van de beleidsmedewerker privacybeleid bij Bureau van de Raad. Tegelijkertijd is er voor gekozen om geen aparte overleggen voor privacycoordinatoren te organiseren, maar aan te sluiten bij het overleg van de BVC’ers (LOBRO). De Procureur Generaal van de Hoge Raad heeft op 2 december 2019 in gesprek met de BVC’ers zijn rol van extern toezichthouder toegelicht.

2.3 Informatievoorziening Privacy

Uit de eerste AVG bijeenkomst van 2019 kwam de vraag van de privacy coördinatoren naar voren dat er nog een coherente informatievoorziening mist. Op dit moment zijn de presentaties van de vorige AVG-bijeenkomsten beschikbaar op een landelijke intropagina. Er zal gezamenlijk met de informatievoorziening van de BVA een vraagbaak worden opgesteld. Informatie en vragen die zijn gesteld aan de helpdesk privacy zijn ondertussen geanalyseerd en er is een overzicht van veel gestelde vragen. Vragen over de vakinhoud kunnen worden gesteld aan het LBVr.

Voor de privacy coördinatoren van de gerechten is een intropagina opgesteld waarop informatie gedeeld kan worden met de gerechten. De privacycoödinatoren kunnen verder via deze intropagina informatie opslaan en onderling uitwisselen. De landelijke projectpagina wordt bijgewerkt, zodra er nieuwe informatie beschikbaar is.

De veel gestelde vragen zullen op de intropagina van de privacycoördinatoren gepubliceerd worden.

Actie:

- Publiceren veel gestelde vragen (beleidsmedewerker privacy Rvdr; 2e kwartaal 2020)

2.4 Register rechtmatige verwerkingen

De rechtmatigheid van verwerkingen bij de landelijke diensten is gecontroleerd bij het vullen van het landelijk register. Er is een inventarisatie geweest van de lokale registers door het AVG projectteam. Het is belangrijk om beter in zicht te brengen of alle verwerkingen bij de lokale registers voldoen aan de AVG. Hiervoor wordt in het 2e kwartaal 2020 een plan van aanpak opgesteld naar aanleiding van de respons via het Key Control Dashboard.

➔ Zie punt 3.1.2

2.5. Bewaartermijnen

Voor de Rechtspraak zijn de bewaartermijnen vastgelegd in zogenoemde 'Basis Selectie Documenten' (BSD). Deze zijn:

- **Het BSD Rechtelijke macht**:
  5.1(2)h [redacted] (een wijziging van dit BSD is in voorbereiding door de mandaatgroep archieven)
- **Het BSD Bedrijfsvoering Rechtspraak (inclusief P-dossier):**
  https://zoek.officielebekendmakingen.nl/stcrt-2018-23197.html

De veranderingen lijken minimaal door komst van de AVG. Vanuit het J&V-Privacy board waarin de privacy officer van IVO participeert namens de Rechtspraak is een memo gedeeld inhoudende uitgangspunten en bewaartermijnen. Op basis van deze richtlijnen dienen de concrete bewaartermijnen per (onderdeel van een) systeem te worden opgetekend. In principe zijn de basisselectiedocumenten zowel voor papier als voor gegevens opgenomen in digitale systemen.

Door de IVO-portefeuillehouder Generieke systemen/Bedrijfsvoering is, in afstemming met medewerkers van het bureau, een advies geformuleerd hoe bewaartermijnen uit de basisselectiedocumenten vertaald zou kunnen worden naar systemen. Dit voorstel zal door de CIO ter besluitvorming worden voorgelegd aan de Raad, nadat het SBO hierover gehoord is.
In het kader van het IV-project AVG zal worden bezien in hoeverre technische hulpmiddelen kunnen bijdragen aan het tijdig vernietigen van gegevens.

Acties:

- Vaststellen concrete bewaartermijnen voor digitale systemen door Raad (2e kwartaal 2020)
- Vertalen naar systemen en processen (IVO en LOV's)
- Inregelen mogelijkheden tot automatisch verschonen (IVO + portefeuillehouders)

Rechtspraakscore:
Oranje (Omdat voor de meeste aspecten wel duidelijk is of er wel of niet rechtmatig wordt verwerkt en er een aanpak ligt om dit geregeld te krijgen).

2.6. Coronacrisis

Naar aanleiding van de verspreiding van COVID-19 heeft het kabinet in maart 2020 verschillende maatregelen afgekondigd. Het gevolg van deze maatregelen is onder andere dat rechtbanken alleen nog open zijn voor urgente zaken en dat het verzuim om verschillende redenen is toegenomen.

COVID-19 noodzaakt de gerechten maatregelen te nemen om ervoor te zorgen dat de bedrijfsvoering zo veel mogelijk doorgaat. De privacywetgeving blijft ook in tijden van crisis gelden en het is van belang dat de gerechten bij het nemen van de maatregelen hier, ondanks de crisis, aan blijven voldoen.

Acties (beleidsmedewerker privacy/FG):

1. welke verwerkingen naar aanleiding van COVID-19 extra plaatsvinden;
2. toetsen of de verwerkingen rechtmatig gebeuren;
3. de gerechten adviseren wanneer gegevens in meer of mindere mate onrechtmatig worden verwerkt.

3. AVG-documentatieplicht

Hierbij wordt gekeken naar de volgende punten: De aanwezigheid van een gevuld verwerkingsregister en indien deze er niet is een plan met einddatum; Het actueel zijn van verwerkersafspraken, indien niet actueel wanneer de verwachte einddatum is om deze actueel te hebben; Het hebben van een PIA proces waarbij de PIA's met de FG worden afgestemd. Indien één van deze punten niet voorhanden is, maar wel een plan met einddatum wordt oranje gescoord, geen plan met einddatum leidt tot rood. Alleen als alle punten op orde zijn wordt groen toegekend.

3.1. Privacy normenkader voor IVO en de gerechten

Vanuit IVO was er de wens om te werken met een privacy normenkader binnen de organisatie. Begin 2019 is onderzocht welk bestaand model het best past bij de organisatie en het oog viel toen op het CIP normenkader. Het model is alleen gebaseerd op de AVG. Hierdoor moet er nog door de Rechtspraak de normen van de WSJG aan worden toegevoegd en aangepast worden op de praktijk van de Rechtspraak. Hieraan wordt op dit moment door de beleidsmedewerker privacy bij de Raad gewerkt.

Er wordt voor het toetsen van privacy binnen de gerechten en landelijke diensten aansluiting gezocht op het Key Control Dashboard, zoals dit al wordt gebruikt voor Financiën en BVA. In september 2019 is er opdracht gegeven aan een externe leverancier tot het uitbreiden van het Key Control Dashboard met een module met normen/vragen t.a.v. privacy.
De BVC'ers kunnen dan via de KCD tool worden bevraagd over de implementatie van de AVG en de Wjsg binnen het gerecht.

Door de directeur van IVO is ondertussen goedkeuring gegeven om de door DJI ingeregelde software voor het maken van PIA's te gaan aanbesteden. In het kader van deze aanbesteding wordt gewerkt aan een PIA.

De KCD tool waar hierboven over wordt gesproken is inmiddels ontwikkeld en geïmplementeerd. Verder zijn er ook andere functionaliteiten in productiegenomen. In april zal de eerste uitvraag naar gerechten en diensten plaatsvinden.

Acties:

- Opstellen en vaststellen privacynormenkader (beleidsmedewerker privacy Rvdr; 2e kwartaal 2020)

3.2. Verwerkersregister

Door de projectleiding van het AVG project van de Rvdr is een landelijk verwerkingenregister opgesteld. In dat kader is gerealiseerd in samenwerking met IVO, gerechten en diensten:

- ✓ Landelijk register: 150+ IT applicaties (beheer IVO);
- ✓ Lokale registers: lokale IT en registraties (beheer gerechten en landelijke diensten zelf);

Een samenvatting is te vinden via: register van verwerkingen

Deze inventarisaties waren 25 mei 2018 (nagenoeg) afgerond. Er zijn landelijke applicaties buiten beschouwing te zijn gelaten en die worden momenteel toegevoegd aan het registers. De Rvdr is als verwerkingsverantwoordelijke verantwoordelijk voor het vullen van het landelijke register. Het bijhouden en verder vullen is echter door de Rvdr gedelegeerd aan de privacy officer van IVO omtrent de verwerkingen die landelijk plaatsvinden, worden uitgevoerd door IVO. Daarnaast is er register voor de lokale verwerkingen van de gerechten, Bureau van de Raad, SSR en LDCR.

3.2.1. Landelijk register
Er is een procesbeschrijving opgesteld voor het verder vullen van het landelijk register. Deze procesbeschrijving is goedgekeurd door de FG en de directie van IVO.

Acties:
- Bijhouden landelijk register (privacy officer IVO; afronding eind 2020)

3.2.2 Lokale registers
Er is een inventarisatie geweest van de lokale registers door het AVG projectteam. Het is belangrijk om beter in zicht te brengen welke informatie we op het moment hebben en of dit voldoet. Hiervoor zal de nieuwe KCD-module worden gebruikt.

Actie:
- beleidsmedewerker privacybeleid (2e kwartaal 2020)

3.3 Verwerkersafspraken
Bij de verwerkersafspraken wordt een onderscheid gemaakt tussen:
- De contracten die afgesloten worden via het LDCR, veelal landelijke contracten
- De contracten afgesloten door IVO
- De contracten afgesloten door de individuele gerechten en diensten

3.3.1 LDCR
Eind december 2018 heeft LDCR in samenspraak met de FG, de privacy officer IVO en een contractjurist van IVO tips besproken om een inhaalslag te maken. Een nieuw werkproces bleek nodig voor de aankoop- of aanbestedingstrajecten waarin een PIA door de opdrachtgever wordt opgesteld en indien dat uit de PIA komt, ook een verwerkersovereenkomst. Op 1 mei 2019 was er een conceptversie van het werkproces beschikbaar. Deze conceptversie is getoetst door betrokkenen (inclusief FG). Er is nu een definitieve versie beschikbaar. Zie de inkooppagina onder AVG documenten het document Proces borging AVG in nieuwe aanbestedingen.

Het nieuwe werkproces vraagt kennis over het opstellen van PIA's bij de gerechten en de privacy coördinatoren. Bij de AVG-bijeenkomst van 27 juni 2019 is door LDCR/inkoop een korte toelichting gegeven. Daarnaast is gevraagd om met inkoop contact op te nemen bij twijfel over privacygegevens in lopende lokale contracten, zodat we hierin kennis kunnen delen.

Verder heeft LDCR/Inkoop aandacht voor landelijke raamovereenkomsten waarbij de operationele processen per gerecht verschillend kunnen zijn. Voor die gevallen behoren per gerecht de processen onder de loep gelegd worden in verband met de AVG-verplichtingen. Het LDCR/Inkoop heeft een inhaalslag gemaakt om qua PIA's en verwerkersovereenkomsten aan de AVG-verplichtingen te voldoen. Er is nog een overeenkomst waarbij voldaan moet worden aan de AVG-verplichten. Voor alle andere landelijke contracten is bepaald of er een PIA moet gebeuren en of een verwerkersovereenkomst moet worden opgesteld. Bij nieuwe overeenkomsten wordt gecontroleerd of een PIA gedaan is en of een verwerkersovereenkomst moet worden opgesteld.

3.3.2. IVO
De resterende verwerkersovereenkomsten worden in orde worden gemaakt. Er dienen nog voor elf diensten verwerkersovereenkomsten te worden getekend. Daarbij dient te worden opgemerkt dat voor sommige diensten gezamenlijk een verwerkersovereenkomst moet worden opgesteld. Er zijn reminders verstuurd, de afdeling inkoop zit er bovenop. Helaas is het niet gelukt om alle overeenkomsten zoals gepland voor eind 2019 op te leveren. De privacy officer van IVO blijft dit nauwgezet volgen en ontvangt maandelijks een update van de contractmanager.

3.3.3. Gerechten
Uit de beveiligingsbenchmark van gerechten 2019 van Motivaction d.d. 29 juli 2019 blijkt dat bij organisaties die te maken hebben met “verwerkers” bijna allemaal een verwerkersovereenkomst die met externe partijen hebben. Dit is alleen niet het geval bij de Rechtbank Rotterdam. Bij acht van de twintig organisaties is dit niet van toepassing.

Van Rechtbank Rotterdam is geen statusupdate ontvangen van de bevinding uit het Motivaction onderzoek

3.3 PIA
Er is een PIA procesbeschrijving opgesteld door IVO. De procesbeschrijving behelst zowel PIA voor nieuwe projecten, bestaande diensten waarvoor nog een PIA moet worden afgesloten alsmede jaarlijkse herijking van PIA’s.

De rechtspraak maakt gebruik van een mix van oudere en nieuwe systemen. Van de oude systemen is in het verleden vaak geen PIA uitgevoerd en de PIA’s, die wel zijn uitgevoerd, zijn veelal niet meer actueel.. Sinds 2016 wordt elk nieuw te ontwikkelen systeem onderworpen aan een PIA. Ondertussen wordt standaard bij nieuwe systemen een PIA gemaakt en is voor nagenoeg alle primaire processystemen in 2019 een PIA opgesteld. Dit ligt op schema.

Het programma Usoft wordt binnen verschillende onderdelen van JenV gebruikt voor het doen van PIA’s. Het zou het proces versnellen door het automatiseren en de kwaliteit verbeteren doordat de tool de gebruiker kennis aanreikt. IVO heeft ondertussen besloten dit ook te gaan gebruiken.

Risico’s met een hoog score die niet gemitigeerd worden, moeten ter advisering worden voorgelegd aan de toezichthouder. IVO komt met een voorstel voor voorafgaande raadpleging waarmee de PIA procesbeschrijving kan worden aangepast.

Acties:
- Voorstel proces voorafgaande raadpleging (Privacy officer, 2e kwartaal 2020)

3.4 AVG-project Rechtspraaksystemen

Ten behoeve van de acties die uitgevoerd (moeten) worden door IVO, is een project gestart waarin aan de compliance op het niveau van de IV-systemen wordt gewerkt. De interactie tussen systemen en de borging op het niveau van de processen wordt afgestemd tussen de opdrachtnemer en de voorzitter van de projectstuurgroep. Daarnaast is er een uitvoeringsplan opgesteld waarin er gedetailleerder wordt in gegaan op de materie per systeemniveau.

Voor de belangrijkste oudere primaire processystemen zijn ondertussen PIA’s opgesteld (zie ook 3.3).

Voor het aanpassen van de systemen zullen er nog een aantal beleidsmatige keuzes gemaakt moeten worden. Dit betreft o.a. t.a.v. bewaartermijnen (zie 2.6) en logging (zie hieronder).

De Wjsg vereist logging van de systemen. Door het ministerie van Justitie en Veiligheid is op 1 januari een KB gepubliceerd waarmee uitstel is verleend van de loggingsverplichting. Binnen IVO moet het interne loggingsbeleid worden aangepast en vastgesteld mede gelet op de Wjsg. De verwachting is dat het beleid in 2020 is aangepast en goedgekeurd. Het loggen van mutatieverwerking kan performance problemen in sommige systemen veroorzaken. Er is al een werkgroep geweest die architectuur heeft geschreven en er zijn eisen vanuit verschillende kanten informatiebeveiliging, privacy en eisen vanuit de business.

Na vaststelling van het beleid kan verder worden geïmplementeerd in de systemen conform het eerdere plan. Er zal een meerjarig plan worden opgesteld om logging op orde te brengen.

Bij het aanpassen van de systemen zal er geen onderscheid gemaakt worden of het proces onder de AVG of onder de Wjsg valt. Dit heeft ertoe geleid dat nog geen systemen (die onder de AVG vallen) zijn aangepast. Overigens lijkt met de huidige aanpak ook de deadline voor de Wjsg-systemen niet haalbaar.

Begin oktober hebben de CIO Rechtspraak en de directeur bureau Raad dit naar de Raad voor de rechtspraak gesignaleerd. Door de CIO wordt nu bezien wat de precieze problematiek is en welke technische oplossingen er zijn. Ook zal bezien moeten worden wat e.e.a. betekent voor de investeringsplanning. Daarnaast zal bezien moeten worden welke preventieve, flankerende maatregelen genomen kunnen worden via bewustzijnsacties en via stringenter autorisatiebeheer.

Naar aanleiding van de collegiale toets is geconstateerd dat rubricering van datalekgevoelige informatie onvoldoende gebeurt. Daarom is richting de gerechtsbesturen geadviseerd dat ze hun verantwoordelijkheid moeten nemen inzake het rubriceren van analoge informatie.
Voor het rubricering van digitale informatie is aan het project AVG de opdracht gegeven om in kaart te brengen wat moet gebeuren om rubriceren van vertrouwelijke en hoog vertrouwelijke data werkbaar te maken. Hierbij is het ook van belang dat de beveiligingsmaatregelen genomen kunnen worden.

Verder werkt het project AVG aan een faseplan. De verwachting is dat dit plan in april wordt afgerond. Op dit moment is het nog wachten op informatie om onduidelijkheden in te vullen.

Het aanpassen van de systemen komt door de coronacrisis langzamer op gang. Het aanpassen van de systemen gebeurt nu met de budgetten die er nog voor de verschillende systemen zijn. Voor grotere onderdelen zal meer budget vrijgemaakt moeten worden. Als voorbeeld kan DIVOS worden gebruikt. Het volledig aanpassen van dit systeem zal rond de 1 miljoen euro kosten. Het is echter ook mogelijk dat voor minder geld een beperkte set aan maatregelen genomen kan worden.

Actie:

- Vaststellen beleid omtrent logging (Raad, voorbereid door IVO; 4^{e} kwartaal)
- Afronden faseplan (IVO/projectleider AVG; april/mei 2020)
- Aanpassen systemen (IVO, projectleider AVG)

<u>Rechtspraakscore:</u>
Rood (Er is op dit moment geen plan met einddatum).

4. AVG-verantwoordingsplicht

Hierbij wordt gekeken naar de volgende twee punten: Een adequaat proces voor het melden van datalekken en aanwezig zijn van een register voor de registratie van datalekken; Het hebben van passende beveiligingsmaatregelen voor de beveiliging van persoonsgegevens. Indien één van de punten (register datalekken of passende beveiligingsmaatregelen) niet op orde is maar wel een plan met einddatum wordt oranje gescoord, geen plan met einddatum leidt tot rood. Alleen als beide punten op orde zijn wordt groen toegekend.

4.1 Procedure datalekken

De procedure voor het melden van datalekken is van kracht sinds de zomer 2016. De beveiligings-coördinatoren c.q. privacy coördinatoren bij gerechten en diensten zijn verantwoordelijk voor uitvoering van de procedure. Het registeren gebeurt door middel van het softwarepakket Classbase. FG zorgt, met hulp van de Medewerker BVA, voor een jaarlijks overzicht ten behoeve van het jaarverslag.

Bij de Rvdr was er een datalekteam waarin de FG en een beleidsadviseur ICT en Recht zitting in namen. Ondertussen is er genoeg ervaring opgedaan in het omgaan met datalekken. De toegevoegde waarde van een specifiek datalekteam is afgenomen. Het datalekteam is daarom opgeheven. Er is begin oktober een nieuw handboek datalekken ter beschikking gekomen. In overleg met de PG Hoge Raad is er een onderdeel opgenomen over wanneer er aan de AP of de PG Hoge Raad moet worden gemeld.

Uit de beveiligingsbenchmark gerechten 2019 d.d. 29 juli 2019 blijkt dat de rechtbanken Den Haag en Rotterdam het afgelopen jaar het vaakst te maken hebben gehad met een datalek het afgelopen jaar, met meer dan 30 keer. Ook bij de CRvB, Hof Arnhem-Leeuwarden, Rechtbank Gelderland en Rechtbank Midden-Nederland heeft vaak een datalek plaats gevonden namelijk 20-30 keer het afgelopen jaar. Uit de benchmark blijkt ook dat alle gerechten en diensten beschikken over een intern werkproces/protocol wie binnen het gerecht/de dienst de datalekken meldt aan de toezichthouder, aan eventuele betrokkenen en wie het incident registreert in Classbase.

Veel van de datalekken hangen samen met het onvoldoende anonimiseren van uitspraken die gepubliceerd worden. Op dit moment is dit nog een handmatig proces. Er worden nu testen gedaan met software om publicaties te anonimiseren. De eerste testen zijn positief.

Het landelijk overleg van BVC-ers, het LOBRO, heeft een inventarisatie opgesteld over hoe er in de gerechten omgegaan wordt met verwerking, registratie en meldingen van datalekken. Uit de cijfers over meldingen blijkt een verschil in aanpak per gerecht. Om te voorkomen dat op grond van verschillende behandelingen per gerecht verkeerde conclusies getrokken kunnen worden en ook bij te dragen aan de juiste interpretatie van de regels, zal het LOBRO een set afspraken opstellen. Deze afspraken dragen dan bij aan uniforme verwerking

Acties:

- Afspraken uniforme verwerking datalekken (LOBRO; eind 2e kwartaal)
- Verder ontwikkelen en implementeren anonimiseringstool (IVO; 2020)

4.2. Informatiebeveiliging

Op het moment wordt er gewerkt met 16 normenkaders voor security opgesteld afgeleid van de BIR 2012 en op een aantal punten verder aangescherpt. IVO draagt bij aan het onderhouden en verbeteren van deze normenkaders die breed binnen de organisatie bekend zijn en worden toegepast. Bij audits worden de normenkaders als basis gebruikt. Daar waar nodig is er intern IVO beleid geformuleerd ter aanvulling en verduidelijking op de normenkaders.

In het laatste kwartaal van 2018 is door IVO een onderzoek gestart naar de wenselijkheid om over te stappen naar de BIO. Daarbij wordt tevens bezien welke BIO-normen niet van toepassing kunnen zijn op de rechtspraak en welke aanvullende rechtspraak specifieke normen er nodig zijn.

De inventarisatie m.b.t. de verschillen tussen de normenkaders en de BIO is uitgevoerd. Het besluit is genomen dat IVO Rechtspraak overstapt naar de BIO. Acties worden ontplooid om de BIO voor de gehele Rechtspraak van toepassing te verklaren.

4.2.1. Informatiebeveiliging landelijke systemen.
In 2019 heeft de actie gelopen om de auditbevindingen t.a.v. informatiebeveiliging op te schonen. Dit heeft geresulteerd dat in 2019 totaal 195 bevindingen zijn afgesloten.
De openstaande bevindingen kunnen geclassificeerdn worden in een 3-tal hoogste gebieden:

- Een veilige **SSL**-verbinding die zorgt voor een gecodeerde verbinding tussen de server en bezoeker
- Een goed **cipher suite** die bepaalt hoe het verkeer tussen een server en een cliënt versleuteld en verwerkt wordt.
- Gebruik van **HTTPS**-protocollen met als doel een veilige uitwisseling van gegevens.

Deze risico's zijn onderkend en worden gemonitored.

Acties:

- Audit bevindingen t.a.v. beveiliging krijgen een hogere prioriteit en worden directer gemonitord (IVO, eind 2020).

4.2.2 Autorisatiebeleid Gerechten
Het autorisatiebeleid is volgens de EY-accountant niet op orde en de belangrijkste bevindingen waren:

- het ontbreken van (uniforme) procedurebeschrijvingen omtrent het toekennen, wijzigen en tijdig ontnemen van rechten in de primaire processystemen;
- het ontbreken van inzicht in welke gebruikers over welke toegangsrechten beschikken in de primaire processystemen;
- het ontbreken van een periodieke controle op de juistheid van de toegekende rechten aan gebruikers in de primaire processystemen.

Op basis van de managementletter van de accountant zijn de Gerechten in december 2018 gevraagd om deze punten op te pakken.

IVO is in 2019 een project gestart waarbij de rechtspraak aansluit op het systeem voor identiteitenmanagement van J&V (SIMS). Dit project is naar verwachting eind 2020 afgerond. De bedoeling is om daarna de stap te maken naar Accesmanagement. Dit zal echter een langdurig traject zijn. Idee was om voor de tussenliggende periode voor de Gerechten tooling voor autorisatiebeheer beschikbaar te stellen. Tot nu toe heeft dit niet tot resultaat geleid.

Om antwoord te kunnen geven op de bevindingen van de accountant is in de beveiligingsbenchmark gerechten 2019 d.d. 29 juli 2019 een aantal vragen gesteld over informatiebeveiliging. Dit heeft geleid tot de volgende bevindingen:

- Na de inwerkingtreding van de AVG wordt er niet bij alle gerechten/instanties voldoende veilig omgegaan met informatie op papier. Bij vier gerechten/instanties is dit niet het geval, namelijk Hof 's-Hertogenbosch, Rechtbank Gelderland, Rechtbank Oost-Brabant en Rechtbank Overijssel
    - Status 2 maart 2020: rechtbank Gelderland meldt dat ze hier 'nee' hebben ingevuld, omdat ze datalekken hebben. Hierdoor zijn ze van oordeel dat niet voldoende veilig wordt omgegaan met informatie op papier.
      Van de andere gerechten zijn geen statusupdates ontvangen.

- Bij negentien van de twintig gerechten/instanties zijn de kritieke processystemen in kaart gebracht. IVO Rechtspraak is de enige instantie waar dit niet het geval is.
    - Status 2 maart 2020: geen veranderde status ontvangen.
- Alle twintig gerechten/instanties hebben maatregelen getroffen om bij langdurige uitval van IT, de meest kritische processen doorgang te laten vinden
- Bij vier gerechten/instanties wordt rechtspraakinformatie verwerkt buiten de digitale rechtspraakomgeving, zoals privé -e-mail accounts of privé laptops. Dit betreft de Centrale Raad van Beroep, Rechtbank Overijssel, Rechtbank Oost-Brabant en Rechtbank Zeeland-West-Brabant.
    - Status 2 maart 2020: de CRvB is bezig om dit risico aan te pakken door medewerkers bewust te maken geen informatie buiten de rechtspraakomgeving te brengen en medewerkers (zoals raadsheer plaatsvervangers) te voorzien van een rechtspraak account en een autorisatie te verlenen voor 2fair.
      Van de andere gerechten zijn geen updates ontvangen.
- Het lokale autorisatiebeheer is niet voldoende accuraat ingericht bij Rechtbank Midden-Nederland, Rechtbank Noord-Holland en Rechtbank Oost-Brabant.
    - Status 2 maart 2020: Rechtbank Midden-Nederland werkt aan een lokaal protocol.
      Van de andere gerechten zijn geen updates ontvangen.
- Zestien gerechten/instanties hebben procedurebeschrijvingen omtrent het toekennen, wijzigen en tijdig ontnemen van rechten in de primaire processystemen. De gerechten/instanties waar dit niet het geval is: Rechtbank Midden-Nederland, Rechtbank Noord-Holland en Rechtbank Overijssel.
    - Status 2 maart 2020: Rechtbank Midden-Nederland werkt aan een lokaal protocol.
      Van de andere gerechten zijn geen updates ontvangen.
- Alle twintig gerechten/instanties hebben inzicht in welke gebruikers over welke toegangsrechten beschikken in de primaire processystemen.
- Bij twaalf van de twintig gerechten/instanties vindt periodieke controle plaats op de juistheid van de toegekende rechten aan gebruikers in de primaire processystemen. Bij Rechtbank Gelderland, Rechtbank Noord-Holland en Rechtbank Noord-Nederland is dit niet het geval.
    - Er zijn geen statusupdates ontvangen.
- Bij zeven van de twintig gerechten/instanties vindt er geen incidentele controle plaats op het gebruik van toegekende rechten. Het betreft hier de CRvB, SSR 1 en 2, Bureau Rvdr, Hof Amsterdam, Rechtbank Midden-Nederland en Rechtbank Overijssel.
    - Status 2 maart 2020: door Rechtbank Midden-Nederland wordt door aan een lokaal autorisatieprotocol gewerkt. Verdere zijn geen statusupdates ontvangen

De bevindingen zijn teruggelegd bij de gerechten, die hierop actie zullen ondernemen.

Acties:

- Nagaan voortgang acties gerechten n.a.v. bevindingen (beleidsmedewerker privacy, 2e kwartaal 2020)

<u>Rechtspraakscore:</u>
Oranje

5. AVG-informatieplicht

Hierbij wordt gekeken naar de aanwezigheid een of meerdere processen voor de rechten van de betrokkenen (inzage, rectificatie en bezwaar proces). Het ontbreken zijn één van de processen en geen plan met einddatum leidt tot rood, niet aanwezig wel een plan met einddatum leidt tot oranje.

De procedure voor het beantwoorden van informatieverzoeken van betrokkenen is doorgevoerd binnen de Rechtspraak. Tijdens de implementatie is het volgende gerealiseerd:

- Procedurebeschrijvingen en modelbrieven zijn aan gerechten en diensten ter beschikking gesteld door het AVG projectteam;
- Gerechten en diensten zijn geïnformeerd over de procedure tijdens een aparte themamiddag;
- Gerechten hebben een eigen coördinator informatieverzoeken die bereikbaar is

Er zijn geen signalen dat er op dit punt nog acties ondernomen dienen te worden.

De rol van landelijk coördinator informatieverzoeken wordt niet opnieuw ingevuld. De ervaringen tot nu toe duiden er op dat deze rol niet langer meerwaarde heeft.

<u>Rechtspraakscore</u>
Groen

Deelbesluit 1 - Datalekken
Document 5

(5E) Borgingsplan Privacy Rechtspraak

Versie 23 september 2020

Inhoud

1. Inleiding

Met dit borgingsplan worden de activiteiten van de Rechtspraak t.a.v. privacy inzichtelijk gemaakt. Deze activiteiten beogen om niet alleen te voldoen aan de verplichtingen van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG), maar ook aan de verplichtingen die voortvloeien uit de Wet justitiële en strafvorderlijke gegevens (Wjsg). Daarbij is het niet alleen van belang dat op een bepaald moment aan de eisen wordt voldaan, maar dat dit ook structureel is geborgd. Bij toekomstige ontwikkelingen binnen de Rechtspraak dient ook aandacht besteed te worden aan privacy.

Dit plan is ingedeeld conform de privacy management KPI's van JenV. Daarnaast is er een categorie overig. In de tekst wordt telkens aangegeven waar de Rechtspraak staat en welke activiteiten de Rechtspraak t.a.v. de betreffende KPI onderneemt. Er wordt afgesloten met een indicatorscore waar de Rechtspraak staat en een ambitieniveau waar de Rechtspraak wil staan. Onder de categorie overig vallen onderwerpen die voor de Rechtspraak van belang zijn, maar geen plek hebben gekregen in de KPI's van JenV.

De werkwijze die bij dit borgingsplan wordt gehanteerd, is dat er sprake is van een plan dat minimaal halfjaarlijks wordt herijkt. Het 1e borgingsplan is door de Raad voor de rechtspraak in januari 2019 vastgesteld. Het 2e borgingsplan bevatte de stand van zaken per 1 mei 2019. Het 3e borgingsplan bevatte de stand van zaken per 1 november 2019. Het 4e borgingsplan bevatte de stand van zaken per 1 maart 2020 en dit 5e borgingsplan bevat de stand per 1 september 2020. De eerste vier borgingsplannen waren gebaseerd op de J&V-indicatoren voor het implementeren van de AVG. Het vijfde borgingsplan is voor het eerst conform de privacy management KPI's van JenV opgesteld.

Dit plan gaat niet in op de activiteiten die door het Landelijk Bureau Vakinhoud rechtspraak (LBVr) worden verricht, waarbij het gaat om de werkzaamheden die liggen in het verlengde van het werk van de rechter. Binnen het LBVr is er een jurist die vakinhoudelijke vragen t.a.v. de AVG coördineert en die secretaris is van de werkgroep AVG vakinhoud. De werkgroep AVG vakinhoud is op verzoek van de LOV's opgericht en bestaat uit experts vanuit de gerechten. De leden beschikken over specifieke vakinhoudelijke AVG-kennis. Ook is er een Wikipagina AVG voor het primaire proces van de rechtspraak, waarin (Europese) jurisprudentie e.d. wordt bijgehouden. Hierop zijn ook de antwoorden op de vakinhoudelijke vragen en een overzicht van veel gestelde vragen raadpleegbaar. Vanzelfsprekend is er wel samenwerking met en uitwisseling van kennis tussen het LBVr en de betrokkenen vanuit (de bedrijfsvoering van) de Rechtspraak.

2. Overall beeld: in-control

Per KPI worden verschillende aandachtspunten behandeld. Deze scoring vindt plaats op twee niveaus: het kwaliteitsniveau en het ambitieniveau. De scoringsniveau's gaan van 1 (laagst) t/m 5 (hoogst). De omschrijving van iedere KPI staat in bijlage 1; de betekenissen van iedere score staat in bijlage 2.

Kwaliteitsniveau
Ieder aandachtspunt krijgt een score voor het kwaliteitsniveau dat past bij de huidige situatie. De score wordt onderbouwd aan de hand van voorbeelden (zoals bestaande afspraken, procedures, processen, diensten en producten). Hieruit moet de passenheid van het aangegeven kwaliteitsniveau blijken.

Ambitieniveau
In relatie tot het kwaliteitsniveau wordt aangegeven wat bij ieder aandachtspunt de ambitie van de Rechtspraak is. Hierbij wordt aangegeven welke acties nodig zijn om tot dat niveau te komen. Aan iedere actie wordt een actiehouder en een deadline gekoppeld, zodat periodiek de voortgang wordt vastgesteld. Tegelijkertijd zorgt een actie ervoor dat privacy wederom aandacht en prioriteit krijgt.

Overall-aanpak
Dit borgingsplan is opgesteld in opdracht van de Raad voor de rechtspraak. Opdrachtnemer is de directeur van het Bureau van de Raad voor de rechtspraak.

De uitvoering van de activiteiten wordt gecoördineerd door een werkgroep met daarin de volgende deelnemers:

- Functionaris gegevensbescherming
- Privacy officer IVO
- Functionarissen privacy
- Teamleider security, privacy & kwaliteit IVO
- Wnd CISO
- Hoofd CIO Office
- Beleidsmedewerker privacy bureau Rvdr
- (senior)adviseurs Recht & ICT afdeling Strategie Bureau Rvdr

Agendalid: stafmedewerker Europees recht Landelijk Bureau Vakinhoud rechtspraak

De daadwerkelijke uitvoering van de activiteiten ligt bij een veel grotere groep medewerkers waarbij medewerkers op het terrein van informatiebeveiliging, service delivery, architectuur, applicatiebeheer, inkoop, portefeuillehouders en de lokale privacycoördinatoren bij de gerechten belangrijke partijen zijn.

Rechtspraakscore Overall:
Met dit borgingsplan heeft het management inzicht in de stand van zaken van de implementatie van de privacywet- en regelgeving. Het Overall kwaliteitsniveau van de Rechtspraak is 3. Dit is een representatieve score met de huidige status van privacy binnen de Rechtspraak. Er is al veel werk verzet, maar er is ook nog genoeg te doen.

Disclaimer
De werkwijze en de scoringsmethode die in het borgingsplan worden gebruikt, zijn gebaseerd op een pilot van JenV. De pilot wordt door de Rechtspraak gebruikt om te bepalen of deze werkwijze voor de Rechtspraak werkbaar is. Er is dan ook nog geen bestuurlijke goedkeuring gegeven op de scores. Nadat de pilotfase is afgerond en door JenV formeel goedkeuring is gegeven op de KPI's, zal het bestuurlijke gesprek worden gevoerd om tot het ambitieniveau voor de Rechtspraak te komen.

3. Privacy administratie

De Privacy Administratie omvat alle aandachtsgebieden voor de verwerkingsverantwoordelijke (daarmee veelal de organisatie duidend) die een rol spelen bij het kunnen aantonen van en verantwoorden over de naleving c.q. het compliant werken aan van privacy wet- en regelgeving (Verantwoordingsplicht).

De KPI Privacy Administratie geeft de verwerkingsverantwoordelijke inzicht in de status quo van de wettelijk verplichte documentatieopbouw voor deze aandachtsgebieden (Documentatieplicht) en laat naar buiten zien wat er zoal op de rit is als onderbouwing voor de door de organisatie gehanteerde zorgvuldigheid in haar omgangsvormen met persoonsgegevens.

1 Register van verwerkingsactiviteiten Hierin ligt de onderbouwing van de rechtmatigheid van verwerkingen vast	
Onderbouwing kwaliteitsniveau:	Voorafgaand aan de inwerkingtreding van de AVG is door de projectleiding van het AVG-project van het Bureau Rvdr een landelijk verwerkingenregister opgesteld. In dat kader is gerealiseerd in samenwerking met IVO, gerechten en diensten: ✓ Landelijk register: 150+ IT applicaties (beheer IVO); ✓ Lokale registers: lokale IT en registraties (beheer gerechten en landelijke diensten zelf). Een samenvatting is te vinden via: register van verwerkingen Deze inventarisaties waren 25 mei 2018 (nagenoeg) afgerond. Er zijn destijds landelijke applicaties buiten beschouwing gelaten. Deze worden momenteel toegevoegd aan het landelijke register. De Rvdr is als verwerkingsverantwoordelijke verantwoordelijk voor het vullen van het landelijke register. Het bijhouden en verder vullen omtrent de verwerkingen die landelijk plaatsvinden is echter door de Rvdr gedelegeerd aan de privacy officer van IVO. **Landelijk register** Het landelijk register van verwerkingen moet nog worden aangevuld met de landelijke applicaties die buiten beschouwing zijn gelaten. Daarna moet deze bijgehouden worden. Hiervoor is een procesbeschrijving opgesteld voor het verder vullen van het landelijk register. Deze procesbeschrijving is goedgekeurd door de FG en de directie van IVO. **Lokale registers** Er is een inventarisatie geweest van de lokale registers door de beleidsmedewerker privacy van het bureau Rvdr om te onderzoeken in hoeverre de lokale registers voldoen aan de geldende privacywetgeving. Hiervoor is de nieuwe KCD-module worden gebruikt. De meeste gerechten en diensten hebben een eerste stap gezet met het register van verwerkingsactiviteiten. Sommige zijn volledig en voorzien in alle vereisten uit de AVG. De meeste registers gaan nu echter alleen in op de lokale verwerking en de persoonsgegevens die daarvoor verwerkt worden. Ze missen de bewaartermijnen, grondslagen, doeleinden en een beschrijving van betrokkenen. De gerechten en diensten zijn via de BVC'ers hierop geattendeerd. Kwaliteitsniveau: gezien het bovenstaande is score 1 het meest passend bij de huidige situatie.

Ambitieniveau:	De eerste taak voor de Rechtspraak is ervoor te zorgen dat alle verwerkingen lokaal en landelijk zijn geïnventariseerd en worden bijgehouden. Hierna kan de vervolgstap gemaakt worden dat overbodige verwerkingen worden beëindigd al is de verwachting dat dit deels zal gebeuren bij de inventarisatiefase. Verwerkingen zullen conform hetgeen in het register staat moeten gaan plaatsvinden. De Rechtspraak heeft (nog) niet de ambitie om een centrale structuur op te zetten voor alle registers van verwerkingsactiviteiten. Ieder gerecht is hier immers zelf verantwoordelijk voor. <u>Ambitieniveau</u>: gezien het bovenstaande is niveau 2 het beoogde kwaliteitsniveau. Hiervoor moet de volgende acties worden uitgevoerd: • Bijhouden landelijk register (privacy officer IVO; afronding eind 2020) • In het tweede kwartaal van 2021 zal de beleidsmedewerker privacy nagaan of de voorgestelde verbeteringen in de lokale registers zijn doorgevoerd (actie beleidsmedewerker privacy; 2e kwartaal 2021). • Gerechten moeten conform het register van verwerkingsactiviteiten gaan handelen. Dit betekent data tijdig vernietigen en autorisaties beperken tot degenen die bij de verwerking genoemd staan. Zij worden hier door de FG op gewezen.
2 DPIA's Hiermee wordt gemonitord dat de aanwezigheid en kwaliteit van de risico-inschattingen van verwerkingen adequaat is, zodat risico's teruggebracht worden naar een voor de verwerkingsverantwoordelijke acceptabel niveau.	
Onderbouwing kwaliteitsniveau:	De status van dit aandachtsniveau wordt uitgesplitst naar de situatie bij IVO Rechtspraak, het LDCR en de gerechten en overige diensten. Hierbij kan opgemerkt worden dat PIA's plaatsvinden conform het Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA). Daarnaast wordt in sommige gevallen gebruik gemaakt van de PIA Light. **IVO Rechtspraak** De Rechtspraak maakt gebruik van een mix van oudere en nieuwe systemen. Deze systemen worden door IVO Rechtspraak beheerd. Van de oude systemen is in het verleden vaak geen PIA uitgevoerd en de PIA's die wel zijn uitgevoerd, zijn veelal niet meer actueel. Sinds 2016 wordt elk nieuw te ontwikkelen systeem onderworpen aan een PIA. Ook voor aanpassingen van bestaande systemen wordt een PIA opgesteld. Ondertussen wordt standaard bij nieuwe systemen een PIA gemaakt en is voor nagenoeg alle primaire processystemen in 2019 een PIA opgesteld. Om het proces voor het uitvoeren van PIA's te borgen is door IVO een PIA procesbeschrijving opgesteld. De procesbeschrijving behelst zowel PIA voor nieuwe projecten, bestaande diensten waarvoor nog een PIA moet worden afgesloten alsmede jaarlijkse herijking van PIA's. Verder werkt IVO aan een aanbestedingstraject voor een PIA tool. Dit zal het PIA-proces versnellen door het automatiseren en de kwaliteit verbeteren doordat de tool de gebruiker kennis aanreikt. Uiteindelijk moet de tool ook door de gerechten gebruikt kunnen worden. Door de directeur van IVO is goedkeuring gegeven om de software voor het maken van PIA's te gaan aanbesteden. In het kader van deze aanbesteding wordt gewerkt aan een PIA.

	LDCR Het LDCR verzorgt onder andere de inkoop van producten en diensten voor gerechten. Voor het overgrote deel van de verwerkingen die worden ingekocht, worden in meer of mindere mate persoonsgegevens verwerkt. Deze verwerkingen moeten conform de privacywet- en regelgeving plaatsvinden. Dit betekent dat met terugwerkende kracht moet worden gecontroleerd dat voor iedere afgenomen dienst een PIA is uitgevoerd en een verwerkersovereenkomst (indien nodig) is afgesloten. Eind december 2018 heeft LDCR in samenspraak met de FG, de privacy officer IVO en een contractjurist van IVO tips gekregen om een inhaalslag te maken. Een nieuw werkproces bleek nodig voor de aankoop- of aanbestedingstrajecten waarvoor een PIA door de opdrachtgever moet worden opgesteld en, indien dat uit de PIA komt, een verwerkersovereenkomst wordt afgesloten. Op 1 mei 2019 was er een conceptversie van het werkproces beschikbaar. Deze conceptversie is getoetst door betrokkenen (inclusief FG). Er is nu een definitieve versie beschikbaar.[1] Het nieuwe werkproces vraagt kennis over het opstellen van PIA's bij de gerechten en de privacy coördinatoren. Bij de AVG-bijeenkomst van 27 juni 2019 is door LDCR/inkoop een korte toelichting gegeven. Daarnaast is gevraagd om met inkoop contact op te nemen bij twijfel over privacygegevens in lopende lokale contracten, zodat we hierin kennis kunnen delen. Verder heeft LDCR/Inkoop een inhaalslag gemaakt om qua PIA's en verwerkersovereenkomsten aan de AVG-verplichtingen te voldoen. Er is nog een overeenkomst waarbij voldaan moet worden aan de AVG-verplichten. Voor alle andere landelijke contracten is bepaald of er een PIA moet plaatsvinden en/of een verwerkersovereenkomst moet worden opgesteld. Bij nieuwe overeenkomsten wordt gecontroleerd of een PIA gedaan is en of een verwerkersovereenkomst moet worden opgesteld **Gerechten en overige diensten** Ieder gerecht heeft een register van lokale verwerkingsactiviteiten (zie hiervoor). Voor ieder van deze lokale verwerkingen zou een PIA moeten zijn uitgevoerd, waaruit onder andere blijkt waarom de persoonsgegevens worden verwerkt, hoe lang de persoonsgegevens worden bewaard en welke systemen worden gebruikt. In april 2020 is via het Key Control Dashboard (KCD) onder andere uitgevraagd in hoeverre de nodige lokale PIA's zijn uitgevoerd. Dit heeft tot waardevolle inzichten geleid over de status van PIA's bij de gerechten. Uit de uitvraag is gebleken dat PIA's nauwelijks plaatsvinden. Privacy coördinatoren hebben behoefte aan een training om de kennis inzake PIA's te bevorderen. De noodzaak en mogelijkheden om hier invulling aan te geven, worden onderzocht. Een verslag is naar het LOBRO verstuurd. Kwaliteitsniveau: op basis van het bovenstaande is niveau 2 het meest passend.
Ambitieniveau:	Bij de gerechten vinden PIA's voor de lokale verwerkingen nauwelijks plaats vanwege een gebrek aan kennis en middelen. Desondanks wordt het overgrote deel van de verwerkingen afdekt met PIA's die door IVO en het LDCR structureel worden gesignaleerd. Indien wordt gesignaleerd dat een

[1] Zie de inkooppagina onder AVG documenten het document Proces borging AVG in nieuwe aanbestedingen.

	PIA nog moet worden uitgevoerd, wordt dit aangegeven bij het betreffende gerecht of zorgt de dienst voor de uitvoering van de PIA. Indien een PIA is uitgevoerd, wordt onvoldoende op de bevindingen geacteerd. Voorts worden PIA's onvoldoende herzien, waardoor het cyclische karakter van privacyrisicomanagement ontbreekt. Ten aanzien van dit eerste punt moeten risico's met een hoge score die niet gemitigeerd worden, ter advisering worden voorgelegd aan de toezichthouder. IVO komt met een voorstel voor voorafgaande raadpleging waarmee de PIA procesbeschrijving kan worden aangepast. Ten aanzien van het tweede punt zorgt de aanschaf van de PIA-tool ervoor dat het uitvoeren van PIA's eenvoudiger wordt en dat er een automatische workflow op basis van de PDCA-cyclus ontstaat. <u>Ambitieniveau:</u> de Rechtspraak beoogt niveau 3 te behalen. Hiervoor moeten de volgende acties worden uitgevoerd: • Voorstel proces voorafgaande raadpleging (Privacy officer, 2e kwartaal 2020) • Aanschaf PIA-tool (IVO, 3e kwartaal 2020) • Inventariseren informatiebehoefte en hoeveelheid PIA's om de gerechten hierbij te ondersteunen (beleidsmedewerker privacy, 4e kwartaal).
3 Toestemmingsregister Binnen dit aandachtspunt gaat het over de aanwezigheid en kwaliteit van registraties waaruit de omgang met toestemming voor het verwerken van persoonsgegevens (en het weer kunnen intrekken daarvan) blijkt.	
Onderbouwing kwaliteitsniveau:	Toestemming is een van de grondslagen op basis waarvan het verwerken van persoonsgegevens rechtmatig is. De toestemming die door betrokkenen wordt gegeven, moet vrij en te achterhalen zijn. De verwerkingen van de Rechtspraak worden echter grotendeels gebaseerd op de grondslagen: wettelijke verplichting (art. 6, lid 1, sub c AVG) en de taak van algemeen belang (art. 6, lid 1 sub e AVG). Desalniettemin wordt toestemming gebruikt als grondslag in geval van innovatieve projecten of bij bedrijfsvoering. De documentatie hiervan vindt lokaal bij ieder gerecht en bij iedere landelijke dienst plaats. Ieder gerecht is hier zelf verantwoordelijk voor. Vanuit het Bureau Rvdr wordt hier niet op toegezien, omdat a) er nauwelijks gebruik gemaakt wordt van de grondslag toestemming b) het onderwerp pas inzichtelijk is gemaakt naar aanleiding van deze KPI's. In deze gevallen wordt toestemming (en het intrekken daarvan) gedocumenteerd. Voor wat betreft de Wjsg is dit een wettelijke verplichting. <u>Kwaliteitsniveau:</u> gezien het bovenstaande is de score 2.
Ambitieniveau:	Voor de Rechtspraak is het van belang dat voor ieder gerecht en voor iedere landelijke dienst te allen tijde duidelijk is bij welke verwerkingen de grondslag toestemming wordt gebruikt en dat het proces hieromtrent vastgelegd en geborgd is. Door de FG wordt hierop toegezien. Of sprake is van de grondslag toestemming zal onder andere moeten blijken uit de lokale registers van verwerkingsactiviteiten.

	Ambitieniveau: gezien het bovenstaande streeft de Rechtspraak naar niveau 3. Actie: • Door het Bureau Rvdr zullen de gerechten en diensten gewezen moeten worden op het belang van een gedegen toestemmingsregister (FG en beleidsmedewerker privacy, 1e kwartaal 2021).
4 Datalekregister De wijze waarop informatiebeveiligingsincidenten worden gedocumenteerd, beheerd en qua afhandeling (waaronder de kwalificatie datalek toekenning) worden bewaakt	
Onderbouwing kwaliteitsniveau:	Sinds de zomer van 2016 is er een procedure voor het melden van datalekken. In oktober 2019 is deze procedure vernieuwd in het handboek datalekken. De beveiligings- en privacy coördinatoren bij gerechten en diensten zijn verantwoordelijk voor de uitvoering van de procedure. Het registeren gebeurt door middel van het softwarepakket Classbase. De FG en de BVA zorgen, met hulp van de Medewerker BVA, voor een jaarlijks overzicht ten behoeve van het jaarverslag. Dit jaarverslag wordt gedeeld met de gerechtsbesturen, zodat zij kennisnemen van de resultaten en de daarop gebaseerde adviezen. Hiermee kan het aantal datalekken en informatiebeveiligingsincidenten worden verminderd. Veel van de datalekken hangen samen met het onvoldoende anonimiseren van uitspraken die gepubliceerd worden. Op dit moment is dit nog een handmatig proces. Door IVO wordt een uitvraag voorbereid. Kwaliteitsniveau: gezien het bovenstaande bevindt de Rechtspraak zich op dit moment op niveau 4.
Ambitieniveau:	Het landelijk overleg van BVC-ers, het LOBRO, heeft een inventarisatie gedaan waaruit blijkt hoe er bij de gerechten omgegaan wordt met verwerking, registratie en meldingen van datalekken. Uit de cijfers over meldingen blijkt een verschil in aanpak per gerecht. Om te voorkomen dat op grond van verschillende behandelingen per gerecht verkeerde conclusies getrokken kunnen worden en ook bij te dragen aan de juiste interpretatie en uitvoering van de regels, zal het LOBRO een set afspraken opstellen. Deze afspraken dragen dan bij aan uniforme verwerking en voorkomen dan onjuiste uitkomsten. Ambitieniveau: de Rechtspraak beoogt haar huidige kwaliteitsniveau te handhaven en te verbeteren, doch niet per se tot niveau 5. Acties: • Afspraken uniforme verwerking datalekken (LOBRO; eind 4e kwartaal) • Uitvragen anonimiseringstool (IVO; 4e kwartaal 2020)
5 Gegevensbeschermingsbeleid Hiermee wordt het voor iedereen binnen de organisatie duidelijk hoe met persoonsgegevens wordt omgegaan.	

Onderbouwing kwaliteitsniveau:	Het privacybeleid wordt binnen de Rechtspraak in meerdere documenten op meerdere niveaus vormgegeven:
	- Strategisch niveau:
	  o Strategisch plan privacy
	  o Beveiligingsbeleid voor de Rechtspraak 2019-2023
	- Tactisch niveau:

	o Minimumnormen beveiliging en privacy (op basis van het CIP-normenkader) o IT-security normen (op basis van de BIO). o Intern beleid (bijv. Privacybeleid IVO) - Operationeel niveau: o Procesbeschrijvingen en best practices Het beleid wordt periodiek herijkt op basis van de PDCA-cyclus. Hieronder wordt verder ingegaan op de minimumnormen privacy, de implementatie van de BIO en de verwerking van persoonsgegevens door HRM, inkoop en externe onderzoeken. **Minimumnormen privacy** Vanuit IVO bestaat al lange tijd de wens om te werken met een privacy normenkader. Nadat een eerder normenkader terzijde werd geschoven, is begin 2019 onderzocht welk bestaand model wel past bij de organisatie. Op basis van dit onderzoek is gekozen voor het CIP-normenkader. In beginsel is dit normenkader alleen gebaseerd op de AVG. Daarom zijn door de Rechtspraak specifieke Wjsg-normen aan het CIP-normenkader toegevoegd. Deze privacynormenkaders zijn sinds december 2019 toegevoegd aan het KCD. De BVC'ers kunnen dan via de KCD tool worden bevraagd over de implementatie van de AVG en de Wjsg binnen het gerecht. **BIO** In het laatste kwartaal van 2018 is door IVO een onderzoek gestart naar de wenselijkheid om over te stappen naar de BIO. De inventarisatie m.b.t. de verschillen tussen de normenkaders en de BIO is uitgevoerd. Nadat IVO Rechtspraak in januari 2020 is overgestapt op de BIO, is ook door de gerechten en andere diensten besloten om over te stappen. Om de gerechten en diensten bij de overgang naar de BIO te ondersteunen, wordt door het Bureau BVA in kaart gebracht wat qua beleid inzake niet-IT-security aangepast moet worden om aan de BIO te voldoen. Hieruit moet blijken waarin de gerechten en diensten moeten worden gefaciliteerd. Verder wordt door IVO geïnventariseerd wat zij aan beleid moet aanpassen of toevoegen om het beleid in lijn te brengen met de BIO. Momenteel wordt een nulmeting uitgevoerd op de dienst om te zien waar de hiaten zitten. Verder wordt de PDCA-cyclus ingericht om in control te komen en te blijven. De BIO wordt per hoofdstuk vertaald naar handreikingen (intern beleid). Logging is daarbij als eerste opgepakt. Er worden sessie gegeven om de BIO kennis op niveau te brengen. Tegelijkertijd wordt het (informatiebeveiligings)beleid actief uitgedragen door het management, maar blijft het nog achterwege voor wat betreft privacy. Ook aan privacyopleidingen wordt nog onvoldoende gedaan. **Verwerking van personeelsgegevens** Door de HRM-afdelingen, Inkoop en externe onderzoekers binnen de Rechtspraak worden veel (vertrouwelijke) persoonsgegevens verwerkt. Het is van belang dat deze gegevens rechtmatig worden verzameld, rechtmatig worden verwerkt en tijdig worden verwijderd.

	Naar aanleiding van signalen dat persoonsgegevens onveilig worden verstuurd is het van belang om hier extra aandacht aan te besteden. Kwaliteitsniveau: op basis van het bovenstaande is 3 het best passende niveau.
Ambitieniveau	Ambitieniveau: niveau 5 is haalbaar voor de Rechtspraak en moet ook de ambitie zijn. Beleid wordt opgesteld, door het bestuur vastgesteld en periodiek herijkt op basis van de PDCA-cyclus. Verbeteringen zijn gelegen in het meer actief uitdragen van het privacybeleid door de besturen en directies en het faciliteren van opleidingen. Dit laatste wordt inmiddels ook in kaart gebracht door de werkgroep 'jij-bent-de-sleutel'. Acties: - Faciliteren van de overstap naar de BIO voor de gerechten met o.a. een trainingstool I-bewustzijn (beleidsmedewerker privacy; 1e kwartaal 2022). - Met de afdelingen HRM, Inkoop en externe onderzoek in gesprek om ervoor te zorgen dat privacy ook bij deze disciplines goed geborgd worden (FG/Adviseur privacy & informatiebeveiliging; 2e kwartaal 2021)
6 Privacyverklaring Met een privacyverklaring wordt de informatieplicht over het verwerken van informatie door de verwerkingsverantwoordelijke naar betrokkenen vormgegeven.	
Onderbouwing kwaliteitsniveau:	Door de Rechtspraak is de algemene privacyverklaring gepubliceerd op rechtspraak.nl. De informatie hierin is uitgesplitst per rechtsgebied. Daarnaast is onlangs op de vacaturepagina van de Rechtspraak een aparte privacyverklaring gepubliceerd. Kwaliteitsniveau: op basis van het bovenstaande is niveau 2 het best passend.
Ambitieniveau:	Het ambitieniveau is 3. Hiervoor moet de Rechtspraak meer grip krijgen op gegevensverwerkingen die naast het primaire proces plaatsvinden, zoals het wervings- en selectietraject. Hierna kan de informatieplicht hierop worden aangepast. De realisatiedatum van deze ambitie is afhankelijk van de samenwerking met o.a. teams HRM, Inkoop en externe onderzoeken. Verder is dit ambitieniveau ook afhankelijk van het werk bij de gerechten. Uiteindelijk zal volgens een cyclisch proces de privacyverklaring worden bijgewerkt. Gezien de datum van de actie in het vorige ambitieniveau, kan een eerste aanpassing verwacht worden in het 2e of 3e kwartaal 2021. Een definitieve einddatum kan niet worden gegeven.

4. Transparantie

De KPI Transparantie geeft aan op welke wijze de verwerkingsverantwoordelijke namens diens organisatie invulling geeft aan het transparantiebeginstel, dat onderdeel uitmaakt van de Rechten van Betrokkenen. Transparantie is een onderdeel van de informatieplicht die op de verwerkingsverantwoordelijke rust en gaat over gepaste openheid over de gehanteerde zorgvuldigheid bij het verwerken van persoonsgegevens. De wijze van informatieverstrekking wordt situationeel bepaald en is een belangenafweging. Dit kan persoonlijk en al dan niet 'just-in-time' (mondeling, brief, aanreiken van flyer, digitaal/internet) of indirect en meer algemeen via een privacyverklaring worden vormgegeven, waarbij vereiste informatie voor betrokkenen op of vanuit één plek vindbaar is dan wel wordt aangeboden. Dit informeren gaat in principe altijd vóóraf aan het verwerken van persoonsgegevens van betrokkenen door of namens de verwerkingsverantwoordelijke. Dat dit heeft plaatsgevonden is aantoonbaar.

1 Inhoud informatie Dit omvat **wat** wordt vastgelegd (instroom) en **waarom**, **wie** er toegang heeft tot deze informatie en/of aan wie en waarom worden welke persoonsgegevens verstrekt (doorstroom) maar ook het aangeven hoe lang persoonsgegevens worden bewaard en **wanneer** en op **welke** wijze deze persoonsgegevens weer worden verwijderd, vernietigd en/of gearchiveerd (uitstroom).	
Onderbouwing kwaliteitsniveau:	Bij dit aandachtspunt gaat het over de informatie die onder andere in de privacyverklaring is opgenomen. Op rechtspraak.nl/privacy worden de 5w- en h- vragen beantwoord onder de veel gestelde vragen. Verder gelden voor de bewaartermijnen van documenten in het primaire proces de basisselectiedocumenten. Deze zijn gepubliceerd op nationaalarchief.nl Gezien het bovenstaande voldoende de Rechtspraak aan kwaliteitsniveau 3.
Ambitieniveau:	Met de aanschaf van de PIA-tool ontstaat een meer structureel proces om privacy te borgen. Dit zal er ook voor zorgen dat de gepubliceerde informatie op basis van de PDCA-cyclus steeds zal worden bijgewerkt. Op dit moment heeft de Rechtspraak ambitieniveau 4.
2 Toegankelijkheid informatie Dit omvat het tijdig, begrijpelijk en gemakkelijk, in duidelijke en eenvoudige taal (zonder juridische jargon en waar van toepassing afgestemd op de doelgroep) verstrekken dan wel waar van toepassing ontsluiten of beschikbaar maken van relevante informatie over verwerkingen van persoonsgegevens aan betrokkenen of belanghebbenden.	
Onderbouwing kwaliteitsniveau:	Voor rechtszoekenden en professionals moet het eenvoudig zijn om informatie te vinden over de wijze waarop de Rechtspraak omgaat met persoonsgegevens. Uit aandachtspunt 6 van de KPI Privacy Administratie is gebleken dat de Rechtspraak op twee verschillende plekken een privacyverklaring heeft gepubliceerd: een algemene op rechtspraak.nl en een verklaring die aansluit bij de sollicitatieprocedure van de Rechtspraak. Mochten betrokkenen geïnteresseerd zijn in meer informatie over de Rechtspraak dan kunnen ze gebruikmaken van de verschillende communicatiekanalen die de Rechtspraak aanbiedt, zoals Facebook, Twitter, Instagram en Whatsapp. Kwaliteitsniveau: gezien het bovenstaande ligt niveau 3 het meest in de rede.

Ambitieniveau:	Net als bij het vorige aandachtspunt zal de privacyverklaring door de nieuwe PIA-tooling continu geüpdatet worden op basis van de behoefte van betrokkenen. Het ambitieniveau is 4.
3 Faciliteren uitoefenen privacy rechten door betrokkenen Transparantie gaat over de eenvoud waarop betrokkenen gebruik kunnen maken van hun privacy rechten	
Onderbouwing kwaliteitsniveau:	De AVG en de Wjsg bieden rechtszoekenden en professionals de mogelijkheid om bepaalde rechten uit te oefenen. Het gaat dan bijvoorbeeld om recht op inzage, het recht van rectificatie en het recht om vergeten te worden. Om deze rechten te faciliteren is op rechtspraak.nl/privacy een procedure gepubliceerd hoe betrokkenen van hun rechten gebruik kunne maken. Voor interne betrokkenen is het een en andere gepubliceerd op Intro. De procedures zijn ingevoerd binnen de Rechtspraak. Tijdens de implementatie is het volgende gerealiseerd: • Procedurebeschrijvingen en modelbrieven zijn aan gerechten en diensten ter beschikking gesteld door het AVG projectteam; • Gerechten en diensten zijn geïnformeerd over de procedure tijdens een aparte themamiddag; • Gerechten hebben een eigen coördinator informatieverzoeken die bereikbaar is Bij inwerkingtreding van de AVG werden de gerechten en diensten door de landelijk coördinator informatieverzoeken ondersteund bij het afhandelen van privacyverzoeken van betrokkenen. Al snel bleek dat de gerechten in staat waren de vragen zelf af te handelen. Vanwege een gebrek aan meerwaarde is de rol nu niet meer ingevuld. Eventuele vragen kunnen gerechten altijd stellen via [redacted]@rechtspraak.nl. Kwaliteitsniveau: op basis van het bovenstaande en de indicatoren is 5 (geoptimaliseerd) het meest passende niveau.
Ambitieniveau:	Er zijn geen signalen dat er op dit punt op korte termijn nog acties ondernomen dienen te worden.

5. Privacy by design (PbD) en Default

De KPI PbD geeft de verwerkingsverantwoordelijke voor zijn organisatie inzicht in de mate waarin rekening wordt gehouden met het kwaliteitsaspect privacy als aandachtspunt bij het ontwikkelen van nieuwe (werk)processen, informatiesystemen en/of beleid of wetgeving. De focus van de KPI PbD ligt daarmee bij het borgen van de belangenbescherming van de betrokkene waar persoonsgegevens van worden verwerkt.	
1 Privacy wordt meegenomen in ontwerpfase PbD omvat het vroegtijdig bij en gedurende de doorlooptijd van nieuwe ontwikkelingen aandacht schenken aan de privacy aandachtsgebieden	
Onderbouwing kwaliteitsniveau:	Privacy meenemen vanaf de ontwerpfase betekent dat in een vroeg stadium moet worden bepaald wat de impact van de nieuwe of gewijzigde gegevensverwerking is op de privacy van rechtszoekenden, professionals en/of interne medewerkers. Dit wordt ook wel privacy by design genoemd. De meeste IT-ontwikkelingen vinden plaats bij IVO Rechtspraak. Voor zover er lokale ontwikkelingen zijn, zal privacy ad hoc aandacht krijgen in de ontwerpfase. Het principe van PbD is bij de gerechten onvoldoende bekend. Desalniettemin betekent dit niet dat er (grote) steken vallen. Diensten en IT-producten worden via de inkoopafdeling van het LDCR of IVO aangeschaft. Bij deze inkoopafdelingen zijn procedures ontwikkeld om privacy te borgen door een PIA uit te voeren en, voor zover nodig, door verwerkersovereenkomsten af te sluiten. Hierdoor wordt bij het aanbesteden van een nieuwe lokale dienst of ontwikkeling de privacy toch op een vroeg stadium in de aanschaf meegenomen. Enkel bij lokale initiatieven zal privacy onvoldoende meegenomen worden. Verder wordt bij IVO privacy by design geïmplementeerd in de ontwikkelprocedures. Bij steeds meer ontwikkelingen wordt privacy by design gebruikt, maar een structurele aanpakt waarbij privacy daadwerkelijk vanaf het begin betrokken is, is nog in ontwikkeling. Hiervoor wordt samengewerkt met de ontwikkelteams. Met terugwerkende kracht worden ook de oude IT-systemen AVG-compliant gemaakt (hierover meer onder aandachtspunt 2 van deze KPI). <u>Kwaliteitsniveau:</u> gezien het bovenstaande is niveau 2 het best passend.
Ambitieniveau:	De gerechten en de landelijke diensten moeten nog groeien in het toepassen van privacy by design. Er zijn ontwikkelingen, maar deze zorgen er nog niet voor dat privacy vanaf het begin al in scope is. Verder ontbreekt nog een cyclische werkwijze waarbij: 1) privacyrisico's vanaf dag één in kaart worden gebracht, 2) de maatregelen ter mitigatie van de risico's tijdens de ontwikkeling worden geïmplementeerd, 3) de maatregelen in het register van verwerkingsactiviteiten worden opgenomen en 4) periodiek gecontroleerd wordt op de effectiviteit van de maatregelen. Dit laatste kan leiden tot eventuele aanpassingen. <u>Ambitieniveau:</u> het ambitieniveau is 3. Hiervoor moeten de volgende acties ontplooit worden:

	- Verder implementeren van privacy by design bij IVO Rechtspraak (IVO) - Voorts zullen de gerechten ondersteund worden in de toepassing van privacy by design bij lokale initiatieven waarbij persoonsgegevens worden verwerkt (beleidsmedewerker privacy, 2e kwartaal 2021).
2 Afwegingen in het kader van beoordeling passende maatregelen PbD betekent het bij ontwikkelingstrajecten gestructureerd aandacht geven aan de beoordeling van wat passend is bij de aard, omvang, context en doel van de verwerking en ook anderszins proportioneel is (bijvoorbeeld kostentechnisch) dan wel subsidiair (kan het verwerken ook op een andere wijze, met minder risico's voor betrokkenen).	
Onderbouwing kwaliteitsniveau:	Bij de verwerking van persoonsgegevens moet sprake zijn van een passend niveau van beveiliging. Dit betekent dat de beveiligingsmaatregelen niet ondermaats zijn of overmaats zijn. Het eerste zou een hoger risico op datalekken betekenen, het tweede dat het beveiligingsstelsel te streng en vaak ook te duur is. Voor dit onderdeel wordt ingegaan op de beveiliging van persoonsgegevens in het algemeen. Dit moet immers gedaan worden op basis van een (privacy)risicoafweging waarbij PbD ook een rol speelt. Kwaliteitsniveau: op dit moment is niveau 2 het meest passend bij de status van de Rechtspraak. Bij het merendeel van de verwerkingen zijn de maatregelen in kaart gebracht en geïmplementeerd. Er is echter nog werk dat opgepakt en gestructureerd moet worden uitgevoerd. Ter bespreking hiervan wordt een onderscheid gemaakt in: rubricering, bewaartermijnen, het wegwerken van auditbevindingen, het project AVG en autorisatiebeheer. Uiteindelijk wordt afgesloten met de kwaliteitsscore. **Rubricering** Naar aanleiding van de collegiale toets is geconstateerd dat rubricering van datalekgevoelige informatie onvoldoende gebeurt. Daarom is richting de gerechtsbesturen geadviseerd dat ze hun verantwoordelijkheid moeten nemen inzake het rubriceren van analoge informatie. Voor het rubriceren van digitale informatie is aan het project AVG de opdracht gegeven om in kaart te brengen wat moet gebeuren om rubriceren van vertrouwelijke en hoog vertrouwelijke data werkbaar te maken. Hierbij is het ook van belang dat de beveiligingsmaatregelen genomen kunnen worden. Hierbij moet rekening gehouden worden met de overgang naar de BIO en de gevolgen daarvan voor het rubricering van informatie. **Bewaartermijnen** Voor de Rechtspraak zijn de bewaartermijnen vastgelegd in zogenoemde 'Basis Selectie Documenten' (BSD). Deze zijn: • Het BSD Rechtelijke macht: 5.1(2)h [redacted] een wijziging van dit BSD is in voorbereiding door de mandaatgroep archieven) • Het BSD Bedrijfsvoering Rechtspraak (inclusief P-dossier): https://zoek.officielebekendmakingen.nl/stcrt-2018-23197.html

	Door het ministerie zijn nieuwe selectielijsten opgesteld. De Rechtspraak zal hierop moeten acteren en zijn eigen selectielijsten aanpassen om in lijn te lopen met het ministerie. Op basis van deze richtlijnen dienen de concrete bewaartermijnen per (onderdeel van een) systeem te worden opgetekend. In principe zijn de basisselectiedocumenten zowel voor papier als voor gegevens opgenomen in digitale systemen. Door de IVO-portefeuillehouder Generieke systemen/Bedrijfsvoering is, in afstemming met medewerkers van het Bureau Rvdr, een advies geformuleerd hoe bewaartermijnen uit de basisselectiedocumenten vertaald zou kunnen worden naar systemen. Dit voorstel is voorgelegd aan het SBO op 25 mei 2020. Het is onduidelijk wat de huidige status van dit document is. In het kader van het IV-project AVG zal worden bezien in hoeverre technische hulpmiddelen kunnen bijdragen aan het tijdig vernietigen van gegevens. **Het wegwerken van auditbevindingen** In 2019 heeft de actie gelopen om de auditbevindingen t.a.v. informatiebeveiliging op te schonen. Dit heeft geresulteerd dat in 2019 totaal 195 bevindingen zijn afgesloten. De afgelopen periode zijn 53 bevindingen weggewerkt. De openstaande bevindingen kunnen geclassificeerd worden in een 3-tal hoogste gebieden: - Een veilige **SSL**-verbinding die zorgt voor een gecodeerde verbinding tussen de server en bezoeker - Een goed **cipher suite** die bepaalt hoe het verkeer tussen een server en een cliënt versleuteld en verwerkt wordt. - Gebruik van **HTTPS**-protocollen met als doel een veilige uitwisseling van gegevens. Deze risico's zijn onderkend en worden gemonitord. **Het Project AVG** Door IVO is een project gestart waarin systemenanalyses worden uitgevoerd om te bepalen welke aanpassingen gerealiseerd moeten worden om ze in lijn te brengen met de geldende privacywetgeving. Uiteindelijk is het dan aan de dienstenmanagers en portefeuillehouders om de aanpassingen in de systemen door te voeren. • Door het project is een faseplan opgesteld waarin er gedetailleerder op de materie per systeemniveau wordt ingegaan. Dit document is op 1 september geaccordeerd door de stuurgroep van het project. • Voor het aanpassen van de systemen zullen er nog een aantal beleidsmatige keuzes gemaakt moeten worden. Dit betreft o.a. t.a.v. bewaartermijnen (zie hierboven) en logging (zie hieronder). Om de maatregelen te kunnen implementeren dient door IVO Rechtspraak Architectuur eerst een adequaat architectuurontwerp opgesteld te worden. Deze waren op 11 augustus 2020 nog niet opgesteld. • Voor Berber en GPS worden in 2020 aanpassingen doorgevoerd. In het faseplan wordt een planning opgenomen voor het aanpassen van (primair proces)systemen. Iedere 6 maanden vindt een actualisatie van de planning plaatst. Het streven is om begin 2022, waar mogelijk, de noodzakelijke systeemaanpassingen afgerond te hebben. *Logging*

	De Wjsg, AVG en UAVG vereisen logging door de systemen. Door het ministerie van Justitie en Veiligheid is op 1 januari 2019 een KB gepubliceerd waarmee uitstel is verleend van de loggingsverplichting. Binnen IVO moet het interne loggingsbeleid worden aangepast en vastgesteld mede gelet op de Wjsg. Op dit moment is het loggingsbeleid nagenoeg gereed. De verwachting is dat het beleid in 2020 zal zijn aangepast en zal zijn goedgekeurd. Het loggen van mutatieverwerking kan performance problemen in sommige systemen veroorzaken. Er is al een werkgroep geweest die architectuur heeft geschreven en er zijn eisen vanuit verschillende kanten informatiebeveiliging, privacy en eisen vanuit de business. Na vaststelling van het beleid kan verder worden geïmplementeerd in de systemen conform het eerdere plan. Er zal een meerjarig plan worden opgesteld om logging op orde te brengen. *Status project* Er zijn nog geen systemen (die onder de AVG vallen) aangepast. Met de huidige aanpak lijkt de deadline voor de Wjsg niet haalbaar. Voor beide onderdelen is geen duidelijke planning beschikbaar. Begin oktober 2019 hebben de CIO Rechtspraak en de directeur Bureau Rvdr de onhaalbaarheid van de Wjsg-deadline naar de Raad voor de rechtspraak gesignaleerd. Door de CIO wordt bezien wat de precieze problematiek is en welke technische oplossingen er zijn. Ook zal bezien moeten worden wat e.e.a. betekent voor de investeringsplanning. Daarnaast zal bezien moeten worden welke preventieve, flankerende maatregelen genomen kunnen worden via bewustzijnsacties en via stringenter autorisatiebeheer. Het aanpassen van de systemen komt door de coronacrisis langzamer op gang. Het aanpassen van de systemen gebeurt nu met de budgetten die er nog voor de verschillende systemen zijn. Voor grotere onderdelen zal meer budget vrijgemaakt moeten worden. **Autorisatiebeheer** Het autorisatiebeleid is volgens de EY-accountant niet op orde en de belangrijkste bevindingen waren: • het ontbreken van (uniforme) procedurebeschrijvingen omtrent het toekennen, wijzigen en tijdig ontnemen van rechten in de primaire processystemen; • het ontbreken van inzicht in welke gebruikers over welke toegangsrechten beschikken in de primaire processystemen; • het ontbreken van een periodieke controle op de juistheid van de toegekende rechten aan gebruikers in de primaire processystemen. Op basis van de managementletter van de accountant is aan zijn de Gerechten in december 2018 gevraagd om deze punten op te pakken. IVO is in 2019 een project gestart waarbij de rechtspraak aansluit op het systeem voor identiteitenmanagement van J&V (SIMS). Dit project is naar verwachting eind 2020 afgerond. Voor beide projecten zijn reeds PIA's uitgevoerd. Op basis van hiervoor genoemde opmerkingen vanuit de accountant om meer aandacht te besteden aan autorisatiebeheer is vanuit het Bureau Rvdr een voorstel gekomen om het reeds in gebruik zijnde programma 'de Informatierotonde' in te zetten om een overzicht van autorisaties te genereren. De gerechten krijgen door middel van de Informatierotonde voor autorisatiebeheer een overzicht over wie

	toegang heeft tot welke systemen en over welke rollen/rechten de betreffende personen beschikken. Aan de hand van het autorisatiekader kan per gerecht worden bekeken of de rollen/rechten overeenstemmen met het kader. De ambitie is om het project voor het einde van het jaar af te ronden. Op basis van de uitkomst kunnen vervolgstappen gezet worden.
Ambitieniveau:	Zoals uit de bespreking hierboven blijkt, is de Rechtspraak goed op weg om de privacy structureel in de organisatie te borgen. Met de acties bij deze KPI ambieert de Rechtspraak te komen tot kwaliteitsniveau 5. Hiermee sluit zij aan bij de voorbeeldfunctie die de Rechtspraak in de maatschappij heeft. Hier wordt een onderscheid gemaakt in: algemeen, rubricering, bewaartermijnen, het wegwerken van auditbevindingen en autorisatiebeheer. **Algemeen** • Opstellen planning en realiseren aanpassingen systemen (IVO Rechtspraak). **Rubriceren** Acties: • Bij de implementatie van de BIO wordt ook gewerkt aan een nieuw rubriceringskader. Dit rubriceringskader moet na afronding gedeeld worden met de gerechten, zodat zij dit kunnen gaan toepassen (beleidsmedewerker privacy en IVO; 1e kwartaal 2022). **Bewaartermijnen** Acties: • Vaststellen concrete bewaartermijnen voor digitale systemen door Raad (4e kwartaal 2020); • Vertalen naar systemen en processen (IVO en LOV's); • Inregelen mogelijkheden tot automatisch verschonen (IVO + portefeuillehouders). **Het wegwerken van auditbevindingen** Acties: • Audit bevindingen t.a.v. beveiliging krijgen een hogere prioriteit en worden directer gemonitord (IVO, eind 2020). **Autorisatiebeheer** Het project wordt gevolgd en ondersteund door de beleidsmedewerker privacy. De PIA voor het project is voorgelegd aan de FG.
3 Privacy by default Bij het beschermen van de persoonlijke levenssfeer van de betrokkene voorop staat bij ontwikkelkeuzen. Dit betekent dat altijd die optie wordt geselecteerd die in potentie de minste impact op de persoonlijke levenssfeer van een betrokkene zal hebben.	
Onderbouwing kwaliteitsniveau:	Privacy by default houdt in dat standaardinstellingen op de minst inbreukmakende manier worden ingesteld. Meer inbreukmakende verwerkingen moeten door betrokkene zelf worden ingesteld. Het privacybewustzijn neemt steeds verder toe en medewerkers stellen steeds vaker vragen waarmee qua privacy rekening gehouden moet worden. Aan de andere kant gebeurt er ook nog veel onder de radar. Bij grote of langdurige (IT-)projecten wordt een PIA uitgevoerd en steeds de vraag gesteld of een

	verwerking met minder gegevens kan plaatsvinden. Veelal wordt hier aan voldaan. Het kwaliteitsniveau is: 2. De reden hiervoor is dat er wordt nagedacht over de verwerking met de minst grote impact, maar nog niet structureel. Tegelijkertijd wordt er ook nagedacht over een juiste borging, maar dit moet nog gerealiseerd worden. Hieraan zal de PIA-tool bijdragen.
Ambitieniveau:	Zoals hierboven blijkt is het ambitieniveau minimaal 3. De Rechtspraak beoogt het bewustwordingsniveau verder te vergroten en privacy by default structureel te borgen. De eerste stap is de PIA tool, zodat PIA's eenvoudiger kunnen worden uitgevoerd. Daarna kan het privacyproces verder geborgd worden. Hiervoor is geen concrete termijn te geven, omdat het afhankelijk is van het privacybewustzijn onder medewerkers.

6. Betrokken partijen

De KPI Betrokken partijen geeft inzicht in de wijze waarop organisatiegrens overschrijdend verkeer van persoonsgegevens is ingeregeld en persoonsgegevens buiten de beheersfeer van de verwerkingsverantwoordelijke en daarmee de organisatie raken. Deze KPI kijkt op persoonsgegevensstromen van en naar betrokken partijen in verwerkingen. De onderbouwing van de rechtmatigheid van dit verwerken is een aspect waar de verwerkingsverantwoordelijke zich over dient uit te spreken en zijn maatregelenmix op moet inregelen. Documenteren hiervan vindt plaats in het register van verwerkingsactiviteiten conform en langs de vereisten van AVG art. 30.	
1 Afspraken maken en overeenkomsten sluiten met gebruik van modellen De taken die een verwerkersverantwoordelijke en een verwerker in kader van de gegevensuitwisseling over en weer hebben worden in het kader van de AVG en de Wjsg vormgegeven door vastlegging van afspraken in (bilaterale of multilaterale) afsprakenkaders en verwerkersovereenkomsten.	
Onderbouwing kwaliteitsniveau:	Een verwerker is een andere juridische entitieit die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke(n). Indien uit de PIA blijkt dat sprake is van een verwerker, moet een verwerkersovereenkomst worden afgesloten. Indien een verwerking wordt uitgevoerd door een organisatie die onder dezelfde juridische entiteit valt, zoals de Staat der Nederlanden, worden privacyafspraken gemaakt. Bij dit onderwerp wordt een onderscheid gemaakt tussen: • De contracten die afgesloten worden via het LDCR, veelal landelijke contracten (de huidige situatie is reeds besproken bij het aandachtspunt DPIA van KPI 'Privacy administratie'. • De contracten afgesloten door IVO • De contracten afgesloten door de individuele gerechten en diensten **IVO** De resterende verwerkersovereenkomsten worden in orde gemaakt. Er dienen nog voor elf diensten verwerkersovereenkomsten te worden getekend. Daarbij dient te worden opgemerkt dat voor sommige diensten gezamenlijk een verwerkersovereenkomst moet worden opgesteld. Er zijn reminders verstuurd, de afdeling inkoop zit er bovenop. Helaas is het niet gelukt om alle overeenkomsten zoals gepland voor eind 2020 op te leveren. **Gerechten** Uit de beveiligingsbenchmark van gerechten 2019 van Motivaction d.d. 29 juli blijkt dat organisaties die te maken hebben met "verwerkers" bijna allemaal een verwerkersovereenkomst met externe partijen hebben. Dit is alleen niet het geval bij de Rechtbank Rotterdam, omdat daarvan geen statusupdate is ontvangen. Bij acht van de twintig organisaties is dit niet van toepassing. Kwaliteitsniveau: 4. Voor de meeste verwerkingen waarbij gegevens naar externe partijen worden verstuurd zijn verwerkersovereenkomsten of privacy-afspraken gemaakt voor zover nodig. Voor verwerkersovereenkomsten worden de ARBIT- of ARVODI-modellen van het Rijk gebruikt.
Ambitieniveau:	Ambitieniveau: 5. De Rechtspraak heeft nog niet voor alle externe datadelingen privacy-afspraken of een verwerkersovereenkomst opgesteld. Wel heeft de Rechtspraak in beeld waarvoor nog overeenkomsten afgesloten moeten worden. Hier wordt aan gewerkt. Acties: • De privacy officer van IVO blijft de ontwikkelingen inzake verwerkingsovereenkomsten en privacyafspraken nauwgezet volgen en ontvangt maandelijks een update van de contractmanager.

	• Bij de volgende KCD-uitvraag zal dit punt meegenomen worden (actie beleidsmedewerker privacy; 1e kwartaal 2021).
2 Documentatie onderlinge verhouding t.a.v. verwerking in keten- of andere samenwerking Is er sprake van gezamenlijke verwerkingsverantwoordelijkheid, wat voorkomt als twee of meerdere partijen doel en middelen van verwerken bepalen, moeten ook de onderlinge verhoudingen tot die verwerking worden gedocumenteerd in de registers van verwerkingsactiviteiten en de (bilaterale of multilaterale) afsprakenkaders.	
Onderbouwing kwaliteitsniveau:	Samenwerkingsverbanden zorgen ervoor dat persoonsgegevens buiten de organisatiemuren worden verwerkt. Deze samenwerkingsverbanden kunnen zich vanuit privacyperspectief op verschillende manieren uiten. Zo valt te denken aan een verwerkingsverantwoordelijke en een of meerdere verwerkers, twee verwerkingsverantwoordelijke die ieder hun eigen doel en middelen bepalen of gezamenlijke verwerkingsverantwoordelijkheid waarbij twee of meer organisaties gezamenlijk persoonsgegevens verwerken. Indien sprake is van een van deze relaties moet worden vastgelegd hoe de onderlinge verantwoordelijkheden zijn geregeld. Gezamenlijke verantwoordelijkheid komt vooral voor in de relatie tussen de Raad voor de rechtspraak en de gerechten. In deze relatie is de onderlinge verhouding vastgelegd in diverse governance documenten. Zo ook voor privacy. Verder zijn er weinig gevallen waarbij sprake is van gezamenlijke verwerkingsverantwoordelijkheid. Bij datadeling tussen twee (niet gezamenlijke) verwerkingsverantwoordelijken worden afspraken gemaakt. Hiervoor zijn procedures opgesteld door het LDCR en IVO. Het kwaliteitsniveau is gezien het bovenstaande 3.
Ambitieniveau:	Op dit moment zijn er geen signalen die nopen tot acties om het kwaliteitsniveau te verhogen.
3 Doorgifte persoonsgegevens aan een derde land Er moet duidelijkheid zijn welke waarborgen er zijn getroffen door de verwerkingsverantwoordelijke opdat het voor natuurlijke personen vereiste beschermingsniveau niet wordt ondermijnd.	
Onderbouwing kwaliteitsniveau:	Van doorgifte van persoonsgegevens aan een derde land is sprake wanneer persoonsgegevens buiten de Europese Economische Ruimte worden verwerkt. Denk hierbij aan het versturen of opslaan van persoonsgegevens in de Verenigde Staten. Binnen de Rechtspraak zijn er 11 applicaties die persoonsgegevens buiten de Europese Economische Ruimte (EER) versturen. Hiervoor zijn verwerkersovereenkomsten opgesteld. Door de vernietiging van het adequaatheidsbesluit (Privacyshield) door het Hof van Justitie van de EU wordt op dit moment door IVO in kaart gebracht wat de impact voor de Rechtspraak is. Op basis van de resultaten worden verdere acties bepaald. Noemenswaardig is nog de relatie met het Gemeenschappelijk Hof van Justitie van de Nederlandse Antillen. Op dit moment vinden nog geen gegevensuitwisselingen plaats tussen de Rechtspraak en het Gemeenschappelijk Hof. Er wordt wel in kaart gebracht welke mogelijkheden er zijn om het Gemeenschappelijk Hof gebruik te laten maken van verschillende faciliteiten die de Rechtspraak intern gebruikt. De privacyrisico's zijn hier duidelijk in beeld. Voorts wordt door het CIO-office gewerkt aan het cloudbeleid. Hiervoor heeft afstemming met het ministerie van Justitie en Veiligheid plaatsgevonden. Dit document moet kaders bieden voor doorgifte van persoonsgegevens naar derde landen.

	Kwaliteitsniveau: 4.
Ambitieniveau:	Wanneer in kaart is gebracht wat de impact van de vernietiging van het Privacyshield is, kan hier actie op worden ondernomen. Daarnaast moet het cloudbeleid verder uitgewerkt worden, zodat duidelijke kaders volgen en richtlijnen uitgewerkt kunnen worden. Dit beleid wordt in samenwerking met JenV opgesteld en moet onder andere bevatten wie bevoegd is om risico's te accepteren. Ambitieniveau: 5.
4 Borgen informatiepositie en uitoefening rechten betrokkenen Voor betrokkenen dient het bestaan van meerdere partijen geen onderscheid op te leveren om zijn rechten als betrokkene te kunnen uitoefenen (het bij elke partij aan kunnen kloppen met vragen over de verwerking) maar ook hoe en door wie invulling wordt gegeven aan de informatieplicht van partijen.	
Onderbouwing kwaliteitsniveau:	Ook wanneer sprake is van een samenwerkingsrelatie (zie 2) moeten de rechten van betrokkenen worden gewaarborgd. Hierover moet het een en ander in de verwerkersovereenkomsten of privayafspraken worden vastgelegd Artikel 8 van de ARBIT- en ARVODI- template welke door de Rechtspraak wordt gebruikt, bepaalt dat de wederpartij zal ondersteunen bij de uitvoering van de rechten van betrokkenen. In dezelfde template wordt steeds opgenomen wie de wederzijdse contactpersonen zijn. Hiermee wordt de mogelijkheid van betrokkenen om de wettelijke rechten uit te oefenen gewaarborgd. Betrokkenen worden niet proactief geïnformeerd over de partijen waarmee de Rechtspraak overeenkomsten heeft afgesloten. Kwaliteitsniveau: 3
Ambitieniveau:	Op dit moment heeft de Rechtspraak nog geen signalen om het kwaliteitsniveau te verhogen.

7. Overige onderwerpen

Bij de J&V-indicatoren werden nog enkele andere punten benoemd die relevant zijn om te blijven monitoren, maar geen plek hebben gekregen in de privacy management KPI's. In dit hoofdstuk worden die onderwerpen voor de volledigheid behandeld.

7.1 Coronacrisis

Naar aanleiding van de verspreiding van COVID-19 heeft het kabinet in maart 2020 verschillende maatregelen afgekondigd. Het gevolg van deze maatregelen is onder andere dat rechtbanken alleen nog open zijn voor urgente zaken en dat het verzuim om verschillende redenen is toegenomen.

COVID-19 noodzaakt de gerechten maatregelen te nemen om ervoor te zorgen dat de bedrijfsvoering zo veel mogelijk doorgaat. De privacywetgeving blijft ook in tijden van crisis gelden en het is van belang dat de gerechten bij het nemen van de maatregelen hieraan, ondanks de crisis, blijven voldoen.

Met de versoepeling van de maatregelen is het ook weer mogelijk voor de gerechten om langzaam meer zittingen te laten plaatsvinden. Hiervoor is het een en ander voorbereid door het CMT, SBO en het LOBRO. Zo krijgt ieder gerecht een eigen register. In dit register wordt zes weken lang bewaard wie als publiek aanwezig is geweest bij een zitting. Bij een eventuele besmetting van een aanwezig persoon kan de Rechtspraak bijdragen aan het contactonderzoek. Op dit proces is een PIA Light uitgevoerd die is voorgelegd aan het PRO.

Acties (beleidsmedewerker privacy/FG; doorlopend gedurende de coronacrisis):

1. welke verwerkingen naar aanleiding van COVID-19 extra plaatsvinden;
2. toetsen of de verwerkingen rechtmatig gebeuren;
3. de gerechten adviseren wanneer gegevens in meer of mindere mate onrechtmatig worden verwerkt.

7.2 Vragen AP sectorbeeld politie en justitie

Door de Autoriteit Persoonsgegevens zijn vragen gesteld aan de Rechtspraak om een beeld te krijgen van de stand van dataprotectie binnen de sector Politie en Justitie. De beantwoording van deze vragen wordt door het Bureau Raad, samen met het privacyteam van IVO, voorbereid. Daarna wordt de beantwoording ter vaststelling voorgelegd aan de Raad.

Bijlage 1 Toelichting privacy management kpi's en kwaliteit

Kritieke Prestatie Indicator	Privacy Administratie
Toelichting	De Privacy Administratie omvat alle aandachtsgebieden voor de verwerkingsverantwoordelijke (daarmee veelal de organisatie duidend) die een rol spelen bij het kunnen aantonen van en verantwoorden over de naleving c.q. het compliant werken aan van privacy wet- en regelgeving (Verantwoordingsplicht). De KPI Privacy Administratie geeft de verwerkingsverantwoordelijke inzicht in de status quo van de wettelijk verplichte documentatieopbouw voor deze aandachtsgebieden (Documentatieplicht) en laat naar buiten zien wat er zoal op de rit is als onderbouwing voor de door de organisatie gehanteerde zorgvuldigheid in haar omgangsvormen met persoonsgegevens. De aandachtsgebieden van de Privacy Administratie laten zich als volgt schetsen: 1. Dit omvat de aanwezigheid en kwaliteit van een **Register van verwerkingsactiviteiten** (ook gebezigde termen: **Verwerkingsregister** of **Register van verwerkingen**) waarin de onderbouwing van de rechtmatigheid van verwerkingen wordt vastgelegd. Met deze IST-registratie worden tekortkomingen in de rechtmatigheid dan wel informatieveiligheid [i]) van die verwerkingen gedocumenteerd (afwijking t.o.v. SOLL-positie). Daarmee kunnen activiteiten om die verbeteringen uit te voeren of naleving van bevindingen nader aandacht vragen, worden geregisseerd. Een bevinding kan zijn dat een verwerking moet worden beëindigd omdat deze niet passend is. Het in de tijd kunnen volgen van de toename van de bescherming van persoonsgegevens binnen verwerkingen waarin veranderingen (veelal verbeteringen) zijn doorgevoerd door opeenvolgende registraties in het verwerkingsregister, maakt het tevens mogelijk het naleven van Privacy by Design bij ontwikkeling van processen, informatiesystemen en/of wetgeving aan te tonen. 2. De aanwezigheid en kwaliteit van de risico inschattingen van verwerkingen op de persoonlijke levenssfeer van betrokkenen (**DPIA's**) is binnen deze KPI een te monitoren aspect. DPIA's worden doorgaans aan het Register van verwerkingsactiviteiten gekoppeld en geven inzicht in risico's die voor dit aandachtsgebied gemitigeerd moeten worden tot een qua risicosetting (kans van manifesteren en impact op de betrokkene) voor de verwerkingsverantwoordelijke acceptabel niveau. 3. Binnen deze KPI gaat het ook over de aanwezigheid en kwaliteit van registraties waaruit de omgang met toestemming voor het verwerken van persoonsgegevens (en het weer kunnen intrekken daarvan) blijkt. Een veel gebezigde maar niet geformaliseerde benaming hiervoor is **Toestemmingsregister**. Vastlegging hiervan kan centraal geregeld zijn, maar ook bij de verwerkingen zelf worden gedocumenteerd. 4. De wijze waarop informatiebeveiligingsincidenten worden gedocumenteerd, beheerd en qua afhandeling (waaronder de kwalificatie datalek toekenning) worden bewaakt. Voor deze laatste registraties zijn meerdere benamingen gangbaar. Naast de term **Datalekkenregister** (wat uiteindelijk slechts voor een deelverzameling van informatiebeveiligingsincidenten kan gelden) wordt de term **Informatiebeveiligingsincidenten register** of **Lessons learned register** gebruikt. In de laatste setting dient dit register het doel om aantoonbaar te leren van incidenten. 5. Intern gericht dient de organisatie te beschikken over **Gegevensbeschermingsbeleid** (privacy beleid) waarmee de wijze waarop de verwerkersverantwoordelijke haar medewerkers instrueert hoe met persoonsgegevens wordt omgegaan wordt uitgedragen.

	6. Extern gericht beschikt de organisatie over een **Privacyverklaring.** Hiermee wordt de informatieplicht over het verwerken door de verwerkersverantwoordelijke naar betrokkenen vormgegeven.
Referentie	• **AVG**: art 5, 6, 7, 9, 30, 33, 34 • **UAVG:** Art. 5, 22, t/m 30 • **Overwegingen**: 33, 39, 50, 8, 31, 40, 41, 50, 44, 45, 46, 47-49, 61, 32-33, 42, 43, 171, 34, 51, 56 • **Handreiking naleving AVG**: Hoofdstukken 3, 4, 6 en 7

Kritieke Prestatie Indicator	**Transparantie**
Toelichting	De KPI Transparantie geeft aan op welke wijze de verwerkingsverantwoordelijke namens diens organisatie invulling geeft aan het transparantiebeginstel, dat onderdeel uitmaakt van de Rechten van Betrokkenen. Transparantie is een onderdeel van de informatieplicht die op de verwerkingsverantwoordelijke rust en gaat over gepaste openheid over de gehanteerde zorgvuldigheid bij het verwerken van persoonsgegevens. De wijze van informatieverstrekking wordt situationeel bepaald en is een belangenafweging. Dit kan persoonlijk en al dan niet 'just-in-time' (mondeling, brief, aanreiken van flyer, digitaal/internet) of indirect en meer algemeen via een privacyverklaring worden vormgegeven, waarbij vereiste informatie voor betrokkenen op of vanuit één plek vindbaar is dan wel wordt aangeboden. Dit informeren gaat in principe altijd vóóraf aan het verwerken van persoonsgegevens van betrokkenen door of namens de verwerkingsverantwoordelijke. Dat dit heeft plaatsgevonden is aantoonbaar. De aandachtsgebieden van Transparantie laten zich als volgt schetsen: 1. Het transparantiebeginsel gaat over hoe de verwerkingsverantwoordelijke ervoor zorgt dat betrokkenen bekend zijn met het door de organisatie verwerken van zijn of haar persoonsgegevens. Het kenbaar maken. Dit omvat duiden **wat** wordt vastgelegd (instroom) en **waarom**, **wie** er toegang heeft tot deze informatie en/of aan wie en waarom worden welke persoonsgegevens verstrekt (doorstroom) maar ook het aangeven hoe lang persoonsgegevens worden bewaard en **wanneer** en op **welke** wijze deze persoonsgegevens weer worden verwijderd, vernietigd en/of gearchiveerd (uitstroom). 2. Transparantie gaat over het toegankelijk zijn van deze informatie. Dit omvat het tijdig, begrijpelijk en gemakkelijk, in duidelijke en eenvoudige taal (zonder juridische jargon en waar van toepassing afgestemd op de doelgroep) verstrekken dan wel waar van toepassing ontsluiten of beschikbaar maken van relevante informatie over verwerkingen van persoons-gegevens aan betrokkenen of belanghebbenden. 3. Transparantie gaat over de eenvoud waarop betrokkenen gebruik kunnen maken van hun privacy rechten. Het faciliteren hiervan omvat het eenvoudig kunnen vinden van informatie over specifieke verwerkingen tot en met het daarover kunnen stellen van vragen conform hun privacy rechten.
Referentie	• **AVG**: art. 12, 13, 14. • **UAVG:** - • **Overwegingen**: 39, 58 en 59 (i.r.t. Art. 12 AVG), 60 t/m 62 (i.r.t. Art. 13 en 14 AVG) en 73 • **Handreiking naleving AVG**: par 3.8

Kritieke Prestatie Indicator	**Privacy by Design (PbD) en Default**
Toelichting	De KPI PbD geeft de verwerkingsverantwoordelijke voor zijn organisatie inzicht in de mate waarin rekening wordt gehouden met het kwaliteitsaspect privacy als aandachtspunt bij het ontwikkelen van nieuwe (werk)processen, informatiesystemen en/of beleid of wetgeving. De focus van de KPI PbD ligt daarmee bij het borgen van de belangenbescherming van de betrokkene waar persoonsgegevens van worden verwerkt. De aandachtsgebieden van Privacy by Design (PbD) en Default laten zich als volgt schetsen: 1. PbD omvat het vroegtijdig bij en gedurende de doorlooptijd van nieuwe ontwikkelingen aandacht schenken aan de privacy aandachtsgebieden. Dit betreft géén andere privacy gerelateerde aandachtsgebieden dan al met de AVG zijn aangereikt! Het gaat om het aantoonbaar kunnen maken in hoeverre de privacy aandachtsgebieden al in het ontwerp en de daaropvolgende ontwikkelfase zijn meegenomen in de totstandkoming van de uiteindelijke maatregelenmix om de verwerking met persoonsgegevens passend te beschermen van een nieuw (werk)proces, informatiesysteem, beleid of wet. Dit betekent dat er binnen deze context afwegingen zijn gemaakt die mogelijk hebben geleid tot andere keuzen met minder risico's voor de persoonlijke levenssfeer van betrokkenen. Mogelijke risico's moeten in een ontwikkeltraject zijn teruggebracht tot een voor de verwerkingsverantwoordelijke acceptabel niveau door het gaan toepassen van passende organisatorische en technische mitigerende maatregelen. Het documenteren hiervan in het register van verwerkingsactiviteiten betekent dat de aantoonbaarheid is geregeld. 2. PbD betekent het bij ontwikkelingstrajecten gestructureerd aandacht geven aan de beoordeling wat passend is bij de aard, omvang, context en doel van de verwerking en ook anderszins proportioneel is (bijvoorbeeld kostentechnisch) dan wel subsidiair (kan het verwerken ook op een andere wijze, met minder risico's voor betrokkenen). Dit impliceert onder andere dat de gevoeligheid van de persoonsgegevens die worden verwerkt, in belangrijke mate bepalend is voor de zwaarte van de maatregelenmix maar soms ook, dat PbD richtinggevende verplichtingen voor de verwerkingsverantwoordelijke kan betekenen voor de uiteindelijke oplossingsrichting. 3. Bij PbD is impliciet inbegrepen, dat bij het beschermen van de persoonlijke levenssfeer van de betrokkene voorop staat bij ontwikkelkeuzen. Dit houdt in dat indien bij het ontwerpen van informatiesystemen, (werk)processen en wetten er ergens keuzen worden voorgelegd of moeten worden gemaakt, hierbij als standaard antwoordwaarde (de waarde die gekozen wordt als er niet bewust gekozen wordt) altijd die optie wordt geselecteerd die in potentie de minste impact op de persoonlijke levenssfeer van een betrokkene zal hebben. Dit principe wordt **Privacy by Default** genoemd.
Referentie	• **AVG**: art 24, 25 • **UAVG:** - • **Overwegingen**: 74 t/m 78 • **Handreiking naleving AVG**: par. 2.4

Kritieke Prestatie Indicator	**Betrokken partijen**
Toelichting	De KPI Betrokken partijen geeft inzicht in de wijze waarop organisatiegrens overschrijdend verkeer van persoonsgegevens is ingeregeld en persoonsgegevens buiten de beheersfeer van de verwerkingsverantwoordelijke en daarmee de organisatie raken. Deze KPI kijkt op persoonsgegevensstromen van en naar betrokken partijen in verwerkingen. De onderbouwing van de rechtmatigheid van dit verwerken is een aspect waar de verwerkingsverantwoordelijke zich over dient uit te spreken en zijn maatregelenmix op moet inregelen. Documenteren hiervan vindt plaats in het register van verwerkingsactiviteiten conform en langs de vereisten van AVG art. 30. De aandachtsgebieden die spelen bij Betrokken partijen laten zich als volgt schetsen: Partijen kijken voor het delen van persoonsgegevens (op voorspraak van de verwerkingsverantwoordelijke, zijnde de organisatie die doel en middelen van verwerken vaststelt) ook naar elkaars belangen en de afspraken die er met elkaar gemaakt moeten worden gemaakt over de taakverdeling binnen deze persoonsgegevensdeling. De taken die een verwerkersverantwoordelijke en een verwerker in dit raakvlak met elkaar vormgeven wordt binnen het kader van de AVG vastgelegd in onderling vastgelegde afsprakenkaders (overheid), verwerkersovereenkomsten (voor overheidsopdrachten worden deze doorgaans conform modellen als ARBIT 2018 of ARVODI 2018 opgesteld) of – in het ultieme geval dat de aandacht voor persoonsgegevens al bij aanvang van de hoofdovereenkomst (van opdracht of verwerving) tussen partijen bestond – als onderdeel van die hoofdovereenkomst. Is er sprake van gezamenlijke verwerkingsverantwoordelijkheid, wat voorkomt als twee of meerdere partijen doel en middelen van verwerken bepalen, moeten ook de onderlinge verhoudingen tot die verwerking worden gedocumenteerd (in ieders register van verwerkingsactiviteiten, maar tevens in de afsprakenkaders). Dit speelt o.a. bij verwerken van persoonsgegevens tussen ketenpartijen. Partijen kijken in deze sfeer tevens naar de ketensamenwerking daarbij, zodanig dat ieders privacy administratie op elkaar aansluit. Een verwerker die zelf zijn middelen kiest om daar vorm aan te geven is daarmee overigens géén gezamenlijk verwerkingsverantwoordelijke. Kernpunt daarvoor ligt in de eindbeslissingsbevoegdheid. Ook doorgifte van persoonsgegevens aan een derde land (landen buiten de EEG) of internationale organisaties hoort tot deze KPI. Voor deze laatste situatie is aandacht voor alle daarbij vereiste waarborgen waaronder doorgifte plaatsvindt zoals adequaatheidsbesluiten, passende waarborgen en, bindende bedrijfsvoorschriften. Er moet duidelijkheid zijn (register van verwerkingsactiviteiten) welke waarborgen er zijn getroffen door de verwerkingsverantwoordelijke opdat het voor natuurlijke personen vereiste beschermingsniveau niet wordt ondermijnd. Er wordt rekening gehouden met de consequenties van de actualiteit van wetgevingskaders die op doorgifte kunnen inwerken (denk aan de recente uitspraak over het onrechtmatig zijn van de Privacy Shield overeenkomst in relatie tot gegevensdeling met Amerikaanse bedrijven). De KPI ziet ook op de mate waarin de verwerkingsverantwoordelijke duidelijkheid heeft over de rolverdeling qua verantwoordelijkheid en heeft daaromtrent verwerkingsafspraken of -overeenkomsten met de andere partij(en) opgesteld. Voor betrokkenen dient het bestaan van meerdere partijen geen onderscheid op te leveren om zijn rechten als betrokkene te kunnen uitoefenen (het bij elke partij aan kunnen kloppen met vragen over de verwerking) maar ook hoe en door wie invulling wordt gegeven aan de

	informatieplicht van partijen. Dat dit transparant voor betrokkenen blijft werken is een verplichting die partijen met elkaar moeten regelen in de verwerkersafspraken.
Referentie	**AVG**: art. 24 t/m 30, art. 44 t/m 50 **UAVG: -** **Overwegingen**: 74-77, 78, 79, 80, 81, 13 en 82, 101-102, 101-109 en 169, 108-109, 110, 111-115, 116 **Handreiking naleving AVG**: par 2.3 en hoofdstuk 8 (doorgifte)

Bijlage 2. Invulformulier KPI aandachtsgebieden

Plaats voor alle zes de aandachtsgebieden van Privacy Administratie het betreffende cijfer (1 t/m 6) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Privacy Administratie**		
Organisatie score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	1. Er is centraal inzicht in (de status van) alle verwerkingen in het register van verwerkingen mogelijk door de FG, waarmee diens adviestaak (art. 35.2) wordt ondersteund. Bewaking op de naleving van maatregelen om tekortkomingen te mitigeren wordt (geautomatiseerd) gestructureerd ondersteund. 2. Er is centraal inzicht in (de status van, waaronder daarbij onder handen zijnde (herijkings)assessments in het kader van de Privacy Management Control Cyclus) voor alle DPIA's mogelijk voor de FG, waarmee diens adviestaak (art. 35.2) wordt ondersteund. 3. De organisatie beschikt over een toestemmingadministratie waaruit te allen tijde kan worden afgeleid wanneer en waarvoor toestemming is gegeven alsmede is ingetrokken. De relatie kan worden gelegd tot op de verwerkingsgerichte handeling waar de toestemming op van toepassing is. 4. Er is een workflow ingericht die de achtergronden van informatiebeveiligingsincidenten bij de bron (de melder) documenteert (en waar mogelijk direct mitigeert), de analyse hiervan (wel/geen (meldenswaardig) datalek) vormgeeft en de beschikbare tijd (max 72 klokuren) zo volledig mogelijk beschikbaar maakt voor de operationele afhandeling van datalekken. 5. Privacy beleid wordt periodiek en structureel binnen de Privacy Management Control Cyclus op de beoogde werking (instrueren van medewerkers omtrent de omgang met persoonsgegevens) herijkt en waar van toepassing aangepast en/of geactualiseerd. 6. Betrokkenen worden op gestructureerde wijze geïnformeerd omtrent het verwerken van hun persoonsgegevens vóórdat er sprake van verwerken is.
	4	Voorspelbaar	1. Het register van verwerkingsactiviteiten kent een nadere onderbouwing van elke verwerking. Op basis hiervan kan de kwaliteit van verwerkingen kan worden bewaakt en kan hierover op elk gewenst inhoudelijk niveau worden gerapporteerd. Het register van verwerkingsactiviteiten biedt hiermee tevens inzicht in de kwalitatieve ontwikkeling van verwerkingen in de tijd (periodieke herijkingen). Logging maakt onderdeel uit van de aandacht van de verwerkingsverantwoordelijke, om desgevraagd de handelingen die met persoonsgegevens zijn verricht tot op een diepgang die de AVG vereist (zie NEN 7513 als goed voorbeeld van een gedegen uitwerking hiervoor), te kunnen verantwoorden. 2. De risicoafweging van DPIA's worden gestructureerd en op eenduidige wijze gedocumenteerd. De naleving van het als actie benoemen, agenderen en door voeren van

			gesignaleerde verbeteringen, wordt bewaakt. De herhaalbaarheid van assessments is groot. Periodiek rapporteren aan management kan (geautomatiseerd) op eenvoudige wijze worden vormgegeven. 3. Er is een centrale registratie van toestemming en de status hiervan kan te allen tijde op verwerkingenniveau worden getoond. 4. Er is een duidelijk en binnen de organisatie geborgd protocol voor de afhandeling van datalekken. Uit de registratie van informatiebeveiligingsincidenten wordt periodiek lering getrokken. Verworven inzichten worden gebruikt in opleidingen voor medewerkers, bijvoorbeeld om dergelijke incidenten in de toekomst waar mogelijk te voorkomen (privacy bewustzijn vergroten) en bij de ontwikkeling van nieuwe (werk)processen, informatie-systemen, beleid en wetgeving. 5. Privacy beleid wordt actief uitgedragen binnen de organisatie, onder andere in opleidingen. 6. De publicatie van een privacyverklaring op internet is aangevuld met situationeel in te zetten informatiemateriaal. Dit materiaal dient om betrokkenen, zodra zij een raakvlak krijgen in een betreffende situatie, op correcte en gestructureerde wijze te informeren omtrent het verwerken van zijn/haar persoonsgegevens en de achtergronden daarvan.
	3	Vastgesteld	1. Het stramien van documenteren van verwerkingen in het register van verwerkingsactiviteiten vergroot de herhaalbaarheid (het herijken). Bovendien maakt het de daartoe vereiste effort (beslag op resources) acceptabel. Hierbij wordt doorontwikkeld aan het gestructureerd en geformaliseerd afhandelen van onderkende tekortkomingen en risico's voor de aandachtsgebieden van AVG art. 30 ergo het compliant werken en kunnen komen tot een verantwoorde maatregelenmix en bewaking van de naleving daarvan. 2. Het documenteren van DPIA's is omgeven met een workflow waarvan de beoordeling (kwaliteit/QA en juridisch) ervan een vast onderdeel uitmaakt. Het beoordelingsresultaat is opgenomen in de documentatie. 3. Verkrijgen en intrekken van toestemming bij verwerkingen wordt waar dit speelt eenduidig vastgelegd. Er wordt op toegezien dat al naar gelang op correcte wijze wordt gehandeld, zoals de verwerking waar toestemming voor nodig was maar die ingetrokken is, staken en daarbij vereiste handelingen verrichten (zoals bijvoorbeeld wissen). 4. Het centraal ondersteunen van incidentenregistratie, beoordeling, kwalificatie en afhandeling (waaronder datalekken) begint vorm te krijgen. 5. Er is een gestructureerd Privacy beleid dat door MT is vastgesteld. Dit beleid wordt actief uitgedragen naar personeel/medewerkers, onder meer via opleidingen. 6. Er is een privacyverklaring beschikbaar. Er wordt gewerkt aan procedures om de informatieplicht nader vorm te geven bij situationele verwerkingen.

	2	Beheerst	1. Er worden lokaal binnen de organisatie handmatig beheerde registraties van verwerkingen bijgehouden conform de AVG art.30 vereisten. De organisatie werkt aan een centrale registratie hiervoor. Bijkomend doel is lokale initiatieven voor dergelijke vastleggingen - waar van toepassing - te kunnen beëindigen. 2. Er wordt op gestructureerde wijze vormgegeven aan het opstellen en beheren van DPIA's op papier, uitgevoerd conform het Model Gegevensbeschermingseffect-beoordeling rijksdienst (PIA). 3. Gegeven toestemming wordt op procesniveau dus situationeel gedocumenteerd, evenals het eventueel weer intrekken hiervan. 4. Er is een situationele datalekkenprocedure. De beoordeling en afhandeling van informatiebeveiligingsincidenten worden ad hoc gevolgd. 5. Privacy beleid bestaat nog niet maar is inmiddels in ontwikkeling. 6. Een privacyverklaring is extern beschikbaar.
	1	Informeel	1. De verwerkingsverantwoordelijke verkeerd nog in de fase van ontdekken hoe efficiënt en effectief vorm te geven aan haar documentatieverplichtingen. De organisatie is hiertoe bezig zijn privacy verplichtingen uit te werken qua context en inhoud alsmede beheerbenadering. Er is op lokaal niveau lokaal een basale vastlegging van verwerkingen aan het ontstaan. 2. DPIA's c.q. risicoassessments worden ad hoc en situationeel op papier uitgevoerd conform het Model Gegevensbeschermingseffectbeoordeling rijksdienst (PIA). 3. Toestemming wordt impliciet aanwezig geacht indien persoonsgegevens worden verwerkt. Er vindt geen registratie van plaats. 4. Registratie en het volgen van informatiebeveiligingsincidenten alsmede de analyse of dit datalekken betreft wordt ad hoc en situationeel (waar het zich voordoet) geregeld. 5. Privacy beleid ontbreekt. 6. Er wordt gewerkt aan een centrale privacyverklaring voor de organisatie.

Plaats voor alle drie de aandachtsgebieden van Transparantie het betreffende cijfer (1 t/m 3) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Transparantie**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	1. Reacties van betrokkenen wordt gestructureerd meegenomen bij het opstellen, herijken, beheer en onderhoud van de communicatie en het informeren van betrokkenen over de verwerking van persoonsgegevens. 2. Betrokken worden altijd geïnformeerd over het verwerken van persoonsgegevens voordat dit plaatsvindt. 3. Betrokkenen kunnen informatie over verwerkingen eenvoudig vinden en worden geholpen om hun vragen daaromtrent te stellen.
	4	Voorspelbaar	1. Periodiek vindt binnen de Privacy Management Control Cyclus verificatie en toetsing plaats van de ingerichte werkwijze en procedures om betrokkenen passend te informeren omtrent (de achtergronden van) verwerkingen. 2. Het tijdig en adequaat informeren van betrokkenen omtrent verwerkingen maakt integraal onderdeel uit van de Privacy Management Control Cyclus. 3. Er is een (online) procedure ingericht voor betrokkenen bij verwerkingen om hun privacy rechten op eenvoudige wijze uit te kunnen oefenen.
	3	Vastgesteld	1. Het informeren van betrokkenen over verwerkingen en welke informatie daarbij wordt verwerkt is eenduidig, formeel en procesmatig vastgelegd. Er is consistentie in de uitvoering. 2. De organisatie beschikt over een privacyverklaring waarmee alle informatie omtrent verwerken door de organisatie namens de verwerkersverantwoordelijke voor betrokkenen op één plaats wordt aangeboden. Er kan eenvoudig nadere inhoudelijke informatie bij en over specifieke verwerkingen aan betrokkenen worden verstrekt. 3. Er zijn - waar proces technisch mogelijk - flyers of anderszins voorzieningen gecreëerd om betrokkenen vooraf te informeren omtrent het verwerken van persoonsgegevens op een zo begrijpelijk mogelijke manier (bijvoorbeeld in meer talen beschikbaar).
	2	Beheerst	1. Binnen de organisatie is vastgelegd wanneer en hoe betrokkenen vooraf worden geïnformeerd en welke informatie wordt verstrekt. 2. Er is duidelijk welke informatie verstrekt moet worden in het kader van de informatieplicht en er wordt gewerkt aan een manier om betrokkenen dit ook aan te reiken. 3. Er wordt gewerkt aan informatiemateriaal dat gebruikt kan worden om betrokkenen te informeren omtrent het verwerken van persoonsgegevens.
	1	Informeel	1. Er wordt gewerkt aan werkvormen voor het informeren van betrokkenen omtrent het verwerken van persoonsgegevens. 2. Of en hoe betrokkene wordt geïnformeerd en welke informatie wordt verstrekt is situationeel en sterk afhankelijk van keuze (en kennis op dit vlak) van de lijnverantwoordelijke binnen de organisatie.

			3. Betrokkenen worden situationeel en ad hoc geïnformeerd omtrent verwerkingen. Het behandelen van een verzoek tot het uitoefenen van een of meer rechten van betrokken vindt op gelijksoortige wijze plaats.

Plaats voor alle drie de aandachtsgebieden van Privacy by Default het betreffende cijfer (1 t/m 3) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Privacy by Design/Default (PbD)**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	1. Voor nieuwe (of vernieuwde c.q. van een grote release voorziene) informatiesystemen, werkprocessen of wetgevingstrajecten is het principe van Privacy by Design en Default doorgevoerd in de maatregelenmix. Het bewaken van de implementatie van deze principes is geborgd binnen de Privacy Management Control Cyclus (op een voor de verwerkingsverantwoordelijke passend niveau) door registratie van de gedurende de ontwikkeling gemaakte privacy afwegingen in het register van verwerkingsactiviteiten. 2. Uit het register van verwerkingsactiviteiten zijn naast de verkozen maatregelenmix tevens de gemaakte afwegingen om tot een oplossingsrichting te komen af te leiden. 3. Voor verwerkingen waarbij keuzeafwegingen moeten worden gemaakt met een mogelijke impact op de persoonlijke levenssfeer van betrokkenen wordt bij het invullen altijd standaard de optie die de minste impact heeft op de betrokkene geselecteerd of er zijn organisatorische waarborgen ingesteld om dit te borgen.
	4	Voorspelbaar	1. Nieuwe verwerkingen worden alleen operationeel doorgevoerd (decharge) als aan alle privacy verplichtingen is voldaan gekenmerkt door aantoonbaarheid vanuit de Privacy Administratie. Dit omvat de maatregelenmix in het kader van Privacy by Design gedurende de ontwikkelfase periodiek geëvalueerd en getoetst is aan de stand der techniek (wat is er mogelijk) en uitvoeringskosten (wat kost dat) afgezet tegen de risico's die met de verwerking gepaard gaat en de aard van de te beschermen persoonsgegevens. 2. In de beschouwing van passende bescherming van persoonsgegevens bij verwerkingen wordt het belang van betrokkenen primair gesteld. Bij selectietrajecten om oplossingen te verwerven is het hier niet aan voldoen een showstopper voor de oplossingsvariant. 3. Er is gestructureerd aandacht voor het belang van bescherming van de persoonlijke levenssfeer van betrokkenen bij verwerkingen.
	3	Vastgesteld	1. Gedurende de gehele looptijd van een project/verwerking wordt periodiek de bescherming van persoonsgegevens gevalideerd voor de oplossingsrichting en daaruit ontleende oplossingsvariant. Deze activiteit wordt gedocumenteerd (aantoonbaar) in het register van verwerkingsactiviteiten op een zodanige wijze dat in het ontwerp van verwerkingen de bescherming van de persoonlijke levenssfeer van betrokkenen op een voor de verwerkingsverantwoordelijke passend niveau is verankerd. 2. De principes van Privacy by Design (vroegtijdig aandacht voor privacy) worden systematisch meegenomen als eis (must haves) in programma van eisen bij het verwerven van informatiesystemen.

			3. De bewaking van keuzeopties in informatiesystemen en processen in relatie tot de bescherming van de belangen van betrokkenen is in organisatorische procedures binnen de organisatie ingebed voor die verwerkingen waar het nog geen geautomatiseerde voorziening van de oplossing is.
	2	Beheerst	1. Aandacht voor privacy by design en default is standaard onderdeel van de projectenaanpak voor de ontwikkeling van processen, informatiesystemen, beleid of wetgeving. Op naleving van het rekening houden met deze privacy aandachts-punten in projecten wordt toegezien en gestuurd. 2. Bij het bepalen van de maatregelenmix rond verwerkingen wordt rekening gehouden met het belang van betrokkenen in het kader van de bescherming van de persoonlijke levenssfeer. 3. Er wordt nagedacht over het bepalen van keuzen met de minst grote impact en de manieren om te borgen dat die standaard als antwoord worden voorgelegd.
	1	Informeel	1. De aandacht voor privacy als aandachtsgebied wordt ad hoc en soms afhankelijk van de kennis hieromtrent binnen het project opgepakt bij het ontwerpen van processen, informatiesystemen of wetgeving. Het documenteren van de afwegingen rondom inrichting van de privacy aandachtsgebieden van verwerkingen is situationeel en nog niet gestructureerd ingericht. 2. De bepaling van de adequaatheid van de maatregelenmix is een open proces zonder duidelijke afwegingskaders. Dit is onderkend en hieraan wordt gewerkt 3. De keuzeopties in informatiesystemen hebben (komend uit de verpakking) een functionele, soms alfabetische of numerieke insteek, maar zijn daarmee niet per definitie een inrichting die passend is vanuit Privacy by Default oogmerk. Dit is onderkend en er wordt onderzocht hoe dat op te lossen.

Plaats voor alle vier de aandachtsgebieden van Betrokken partijen het betreffende cijfer (1 t/m 4) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Betrokken partijen**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	1. De afsprakenkaders voor het verwerken van persoonsgegevens zijn voor elke verwerking die hiervoor in aanmerking komt tussen de partijen afgestemd en op passende wijze aantoonbaar gedocumenteerd en actueel. 2. Bij delen van persoonsgegevens buiten de organisatiegrenzen worden de onderlinge verhoudingen (verwerkingsverantwoordelijke, verwerker, gezamenlijk verwerkingsverantwoordelijk) periodiek (binnen de Privacy Management Control Cyclus van 3 jaar) herijkt. 3. Er is een duidelijk kader en/of richtlijnen en vastgelegde structuur voor levering van persoonsgegevens met derde landen beschikbaar, die het vereiste beschermingsniveau van persoonsgegevens hierbij borgt. 4. Het hoger management stuurt op het volgens beleid correct verwerken van persoonsgegevens en monitort daarbij de naleving van de belangen van betrokkenen.
	4	Voorspelbaar	1. De afsprakenkaders tussen partijen zijn helder, effectief en efficiënt vastgelegd in daartoe geëigende en met elkaar vastgestelde formele documenten. 2. De onderlinge verhoudingen tussen de partijen is eenduidig met elkaar overeengekomen en gedocumenteerd. 3. Er is bij internationale doorgifte structureel aandacht voor het belang van de impact van adequaatheidsbeslissingen op de (on)rechtmatigheid van verwerkingen. Er vindt sturing plaats op de toepassing van het centraal bepaalde beleid m.b.t. vastlegging en vaststelling van de grond van de verder verwerking. 4. De wijze waarop invulling gegeven wordt aan de rechten van betrokkenen en het informeren over verwerkingen van betrokken is vastgelegd in processen.
	3	Vastgesteld	1. Er is duidelijk hoe verantwoordelijkheden liggen; eenzijdige verwerkingsverantwoordelijkheid, gezamenlijke verwerkingsverantwoordelijkheid, verwerker. 2. Samenwerking tussen partijen is gestructureerd en erop gericht om met elkaar tot gepaste afspraken te komen voor de beoogde deling van persoonsgegevens. 3. De verwerkingsverantwoordelijke verkent de consequenties van internationaal delen van persoonsgegevens voor verwerkingen voor de organisatie. 4. De bewaking en administratie van de verdere verwerking, inclusief de vastgelegde en vastgestelde gronden vinden plaats op organisatieniveau. Van verwerken van persoonsgegevens in relatie tot andere partijen is de rechtmatigheid vastgesteld en dit kan worden aantonen voor betrokkenen.

	2	Beheerst	1. Taken en verantwoordelijkheden van partijen bij verwerkingen worden structureel en gezamenlijk/in overleg geanalyseerd en beschreven. Bij het delen van persoonsgegevens tussen partijen wordt gewerkt met verwerkersafspraken (binnen de overheid) of verwerkersovereenkomsten (externe partijen). Vastleggen en stellen van doelen en beschermingsniveau geschiedt voor iedere verdere verwerking. 2. Reikwijdte en impact van kaders voor gegevensdelen zoals het adequaatheidsbeginsel of het memorandum van overeenstemming en de relatie hiervan met bijvoorbeeld de afdwingbaarheid van afspraken en onderbouwing van redenen van verwerken worden beschouwd. 3. Er vindt analyse plaats van verwerkingen binnen de organisatie waarin sprake is van doorgifte aan derde landen en/of internationale organisaties. 4. De bewaking van persoonsgegevens worden verwerkt volgens vastgelegde gronden en vindt plaats op afdelingsniveau.
	1	Informeel	1. De (werk)relatie tussen partijen is impliciet bepaald in het operationeel werkproces op basis van zich manifesterende situaties. 2. Taken en verantwoordelijkheden tussen partijen van verwerkingen zijn incidenteel beschreven. 3. Er is geen sprake van gegevenslevering aan landen buiten de EEG. 4. Er is georganiseerd dat betrokkenen namens verwerkingsverantwoordelijke worden geïnformeerd over verwerkingen van en door de organisatie, waarbij derden een raakvlak hebben in de verwerking.

Deelbesluit 1 - Datalekken
Document 6

datum	28 januari 2020
datum overleg	23 januari 2020
aanwezig	[redacted] Olav Welling (OW)
Afwezig	[redacted]

Verslag werkgroep privacy 23-1-2020

1. Opening/mededelingen

OW opent de vergadering en heet iedereen welkom.
De agenda wordt zonder aanpassingen goedgekeurd.
[redacted] stelt zichzelf voor. Hij werkt sinds kort als Functionaris Privacy bij IVO.

2. Vaststellen verslag 17 november 2019

Het verslag wordt zonder aanpassingen vastgesteld.

3. Actualisatie borgingsplan

Het borgingsplan wordt per 1 maart weert geactualiseerd. [redacted] heeft daarom het borgingsplan van november 2019 rondgestuurd met het verzoek om een update te geven op de actiepunten.

OW geeft aan dat met het passeren van de tijd er nieuwe onderwerpen naar boven komen die opgenomen moeten worden in het borgingsplan. Een daarvan zijn inzageverzoeken naar BRP-bevragingen vanuit de gerechten. Hiervoor is nu geen duidelijke procesbeschrijving. Dit zorgt ervoor dat het proces lang duurt.

[redacted] licht het plan rondom rubricering toe naar aanleiding van de memo over het HagaZiekenhuis en het onderzoek van de Autoriteit Persoonsgegevens bij de Belastingdienst. [redacted] zal dit gaan bespreken met de projectleider van het project AVG bij IVO. **Dit punt zal opgenomen worden in het borgingsplan**.

Verder koppelt OW terug wat gedurende het overleg met de Procureur-Generaal bij de Hoge Raad besproken is. 5.2 [redacted] In het overleg is een toelichting gegeven waar we als Rechtspraak aan werken. [redacted] vult de rol van FG in totdat een nieuwe FG gevonden is.

5.2 [redacted]

Tot slot wordt het geactualiseerde borgingsplan van 1 maart naar de PG gestuurd.

4. Visie inzake het gebruik van clouddiensten

[redacted] werkt aan een cloudbeleid. Daarna wordt een cloudstrategie opgesteld. Op dit moment bevindt zich al redelijk wat informatie in de cloud. Beoogd wordt om het document eind maart/ begin april af te ronden, zodat het document goedgekeurd kan worden. De behoefte aan cloudbeleid is groot en actueel. Verschillende diensten worden al in de cloud aangeboden en er wordt beoogd andere diensten via de cloudleveranciers te gaan aanbieden.

[redacted]

5. Leaflet datalekken

[redacted] nadat vanuit Rechtbank Midden-Nederland gesignaleerd is dat het leaflet datalekken door de tijd is ingehaald, is door [redacted] een voorstel gedaan voor een geactualiseerd leaflet datalekken.

Op basis van het nieuwe leaflet vindt een discussie plaats wie meldt bij betrokkene en wie meldt aan de toezichthouder. Er o.a. gevraagd of er een concreet mandaatbesluit is waaruit blijkt dat de landelijke diensten zelf datalekken melden. [redacted] heeft hier geen antwoord op en zoekt dit samen met OW en [redacted] uit. Bij de Autoriteit Persoonsgegeven is gemeld dat landelijke diensten mogen melden.

Verdere opmerkingen op de leaflet:

- AP/PG moet aangepast worden in de tabel
- De bestuurlijke beroepscolleges melden bij een aparte toezichthouder

Actie: [redacted] doet een voorstel voor in het Handboek en de leaflet en bespreekt dit met [redacted]

6. Terugkoppeling gesprek PG HR

Onderwerp is reeds besproken bij de actualisering van het borgingsplan.

7. Voorafgaande raadpleging

[redacted] heeft enkele PIA's bestudeerd. Hierbij constateert hij dat er nooit is gekeken naar voorafgaande raadpleging, zoals opgenomen is de AVG. Dit had bijvoorbeeld gedaan moeten worden bij het accepteren van een risico in Berber waarbij overmatig data werd verstuurd.

[redacted] en [redacted] geven aan bij de PIA betrokken te zijn geweest. Het risico is toen onderkend, maar er is toen nooit sprake geweest van acceptatie van dit risico. In de PIA is toen ook een mitigeerde maatregel opgenomen.

Verder is bij de PIA van Zivver sprake geweest van voorafgaande raadpleging door het betrekken van de PG.

De aanwezigen vinden het goed dat [redacted] dit aangeeft. Voorafgaande raadpleging is een legitiem vraagstuk en moet dan ook voorkomen in de PIA. Voor Berber moet uitgezocht worden hoe het proces van acceptatie is doorlopen en of acceptatie op het juiste niveau heeft plaatsgevonden. Tot slot moet

antwoord komen op de vraag hoe de verantwoordelijkheden voor het accepteren van privacyrisico's liggen rondom IT-projecten.

Actie: vanuit IVO en [redacted] werken samen aan een voorstel voor voorafgaande raadpleging. Deze kan opgenomen worden in de procesbeschrijving PIA bij IVO. **Dit punt wordt als actiepunt in het borgingsplan opgenomen.**

Actie: IVO gaat na hoe en door wie het hoge risico in Berber is geaccepteerd. Eventueel worden hier aanvullende acties op ondernomen.

8. Privacy-bewustwordingsacties

OW vraagt zich af of de bewustwordingsacties voldoende geborgd zijn.
[redacted] geeft aan dat vanuit JenV een traject gestart is voor een e-learning tool. Hier doet de Rechtspraak niet aan mee. Het is onduidelijk of dit is een bewuste keuze is geweest. Met deze e-learning tool kunnen we actiever zijn dan met posters.
OW stelt de vraag wat vanuit SSR als awareness training aangeboden wordt en in welke mate privacy voldoende in de cursussen geborgd is.
[redacted] geeft aan dat bewustwording structureel geregeld moet worden onder de vlag van de FG.
[redacted] geeft aan dat IVO een roadmap heeft opgesteld om bewustwording verder te organiseren. Deze wordt te zijner tijd opgestuurd. Verder geeft [redacted] aan dat het goed is om dit onderwerp op te pakken samen met de andere Wjsg privacy officers.

Op 24 februari is er een sessie van de werkgroep 'jij bent de sleutel'.
[redacted] stelt voor om het bewustwordingsspel over te dragen aan het opleidingsteam van IVO, zodat dit een structureel karakter krijgt en als training aangeboden kan worden.

Tot slot is er nog geen invulling gegeven aan de rol van privacy officer bij het LDCR, zodat bewustwording hier wordt geborgd.

Actie: [redacted] kijkt wat ze kan regelen met de privacy officers die onder de Wjsg vallen. [redacted] neemt privacy mee als input voor de werkgroep 'jij bent de sleutel'.
Actie: [redacted] vraagt de meest recente PIA bij het LDCR.

9. Vacature FG

OW geeft aan dat er een behoorlijk aantal sollicitanten is. Olav neemt de privacykant bij de gesprekken waar.

10. WVTTK/ Rondvraag

Er zijn geen vragen voor de rondvraag

11. Sluiting

Olav sluit de vergadering. Hij zorgt dat er voor de tweede week van maart een nieuw overleg wordt gepland.

Deelbesluit 1 - Datalekken
Document 7

datum	20 juli 2020
datum overleg	16 juli 2020
aanwezig	[redacted] Olav Welling (OW); [redacted]
Afwezig	

Verslag werkgroep privacy 16 juli 2020

1. **Opening/mededelingen**
   Het overleg wordt door OW geopend.

   Door [redacted] wordt de mededeling gedaan dat de Rechtspraak vanuit het ministerie andere KPI's gaat krijgen om de privacyvoortgang mee te bewaken. De scoring zal bestaan uit 5 volwassenheidsniveaus. [redacted] zal de KPI's doorsturen als ze deze heeft ontvangen.
   OW geeft aan dat het verstandig is om hiermee bij de volgende herziening van het borgingsplan rekening te houden.

2. **Vaststellen verslag 20 mei 2020**
   Het verslag wordt zonder aanpassingen aangenomen.

3. **Actielijst**

- Het actiepunt over de TBV's staat vandaag op de agenda.
- Het actiepunt om Herma te informeren over de status van en het proces voor de Wjsg is afgerond.
- Het punt inzake het bespreken van de privacyverklaring sollicitanten is nagenoeg afgerond. OW stelt voor om het proces (zonder te kijken naar eerder opgeslagen documenten) door te sturen naar de andere HR-teams in het land. Hiervoor worden twee kanalen gekozen:
  - via de privacycoördinatoren bij de gerechten;
  - naar landelijk HRM (via [redacted]

4. **Actualiseren borgingsplan per augustus 2020**
   In augustus wordt weer gekeken hoe het staat met de actiepunten in het borgingsplan. Iedereen wordt gevraagd tijdig informatie aan te leveren. Ditmaal worden ook de volwassenheidsniveaus al meegenomen. OW geeft aan dat we als Rechtspraak realistisch moeten zijn en eerlijk moeten kijken naar de stand van zaken.

   [redacted] zal de update van het borgingsplan ook neerleggen bij de AVG-stuurgroep, zodat zij met een reactie kunnen komen. Verder geeft [redacted] aan dat ze uit de stuurgroep is gestapt.

   Tot slot geeft [redacted] aan dat het streefniveau moet worden bepaald.

5. CISO-functie bij IVO

[redacted] legt de situatie uit. De IVO-directie beoogt de CISO-rol te combineren met de rol van teamleider SP&K. Deze combifunctie wordt dan geplaatst onder de directeur IT. 5.2 [redacted].

[redacted] licht het proces toe dat de IVO-directie heeft gevolgd om tot een besluit te komen. Als kwartiermaker heeft [redacted] met stakeholders een voorstel geschreven met daarin het advies om heel SP&K inclusief CISO te positioneren onder de CIO. De teamleider SP&K en de CISO zijn in het voorstel twee aparte functies. De IVO-directie heeft uiteindelijk anders besloten. De reden hiervoor is dat door de herpositionering een reorganisatie zou komen, terwijl de IVO-directie rust wil uitstralen.

5.2 [redacted]

[redacted]

[redacted]

6. Eerste overzicht taken, verantwoordelijkheden en bevoegdheden privacy

[redacted] ligt het agendapunt toe. Het gaat om een eerste overzicht om de taken, verantwoordelijkheden en bevoegdheden inzake privacy binnen de Rechtspraak vast te leggen. Het gaat in dit geval of er fundamentele bezwaren zijn tegen het voorstel.

Er zijn geen fundamentele bezwaren. Er worden wel tips geven:

- Om te zorgen dat het overzicht duidelijk blijft, moet in een rij niet meer dan een E staan.
- Verdeel de lijst in categorieën om lange lijsten te voorkomen.

[redacted] en [redacted] geven beide aan dat er meer tekst ter ondersteuning van de tabel moet komen. Verder stelt [redacted] voor om [redacted] te betrekken bij dit overzicht.

7. Prejudiciële vragen: taak van de rechter

[redacted] ligt het agendapunt toe. Door de rechtbank Midden-Nederland zijn naar aanleiding van een zaak prejudiciële vragen aan het HvJ EU gesteld over de reikwijdte van de competentie van de verschillende toezichthouders in Nederland.
De Rechtspraak stelt zich terughoudend op. Het pleidooi dat waarschijnlijk naar het HvJ EU gaat, is vergelijkbaar met de wensen van de Rechtspraak.

8. Werkgroep openbaarheid (o.a. livestreaming en privacy)

[redacted] ligt het punt toe. De leden van de werkgroep hebben de documenten voor dit punt reeds ontvangen.

[redacted] geeft aan dat er een PIA livestreaming opgesteld gaat worden, maar dat deze pas uitgevoerd gaat worden als de tooling in beeld is. De PIA telehoren zal eveneens bij dit traject betrokken worden.

OW stelt voor om te kijken hoe livestreaming bij de Eerste Kamer en de Tweede Kamer wordt geregeld. [redacted] geeft aan dat deze situatie niet helemaal hetzelfde is. Kamerleden hebben immers bewust voor een openbare rol gekozen. Tegelijkertijd kan navragen geen kwaad.

OW geeft aan dat er geëvalueerd gaat worden op basis van eerdere livestreams. Straf zal, met uitzondering van voorleesvonnissen, niet beschikbaar worden gesteld via livestreams.

Dan komt het onderwerp online publiceren van uitspraken nog ter sprake. [redacted] geeft aan dat er veel stukken zijn uitgewisseld tussen de HR, Rechtspraak en de RvS. Deze zullen worden geconsolideerd. De wens is om de resultaten in september te bekrachtigen. De boodschap wordt naar verwachting dat een wettelijke regeling wenselijk is.

[redacted] wijst op de anonimiseringstool die aangeschaft gaat worden.

Verder wordt nog met andere landen contact opgenomen om te kijken hoe daar omgegaan wordt met online publicatie van uitspraken. Van belang is dat de duidelijkheid van uitspraken als minimum gehandhaafd moet worden.

OW wijst tot slot op een tweetal uitspraken:
- Een rechtbank beveelt het publiceren van de uitspraak inclusief foto.

- Uitspraak wrakingskamer viruswaanzin: de wrakingskamer heeft de beelden van de zitting bekeken om mede te bepalen of er sprake was van partijdigheid.

9. Standaard excuusbrief bij informeren betrokkenen

Naar aanleiding van een datalek wil [redacted] een voorstel doen van een standaard excuusbrief. Deze excuusbrief bevat tekstblokken die in geval een datalek gebruikt kunnen worden.

De aanwezigen zijn het eens met dit voorstel. Daarnaast is het ook wenselijk dat er bij een datalek altijd sprake is van persoonlijk contact. Dit bevordert de relatie met de burger. Na het telefoongesprek kan dan op papier worden vastgelegd wat besproken is.

OW geeft twee tips:
- er kan gebruikt gemaakt worden van Schrijfhulp.
- vraag bij klachtenteams na hoe zij hiermee omgaan.

10. WVTTK/ Rondvraag

[redacted] geeft aan dat het HvJ EU uitspraak heeft gedaan in de Schrems II zaak. Het HvJ EU heeft het adequaatheidsbesluit tussen de EU en de VS vernietigd. Er wordt nu in kaart gebracht wat dit betekent voor de verwerkingen binnen IVO, zoals Zivver en de huisstijl. Daarnaast geeft [redacted] aan dat ook gekeken moet worden naar de impact van deze uitspraak voor het cloudbeleid.

5.2 [redacted]

[redacted] geeft verder aan dat de Kamer voor het notariaat en de Accountantskamer bij haar op de lijn zijn gekomen. Ze vragen zich af wat ze moeten doen wanneer een datalek gemeld moet worden. [redacted] werkt aan een brief richting de PGHR met het verzoek hierin mee te denken. Verder vraagt ook het medisch tuchtcollege zich af hoe ze hiermee moet omgaan. Als iemand ideeën heeft, laat het vooral weten.

11. Sluiting

OW sluit de vergadering.
[redacted] laat de volgende vergadering inplannen rond 1 september.

Deelbesluit 1 - Datalekken
Document 8

(6E) Borgingsplan Privacy Rechtspraak

Versie 01 februari 2021

Inhoud

1. Inleiding

Aanleiding

Het uitgangspunt van de Rechtspraak ten aanzien van privacy is om altijd in lijn met de geldende wet- en regelgeving te handelen. Dit kader wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), Wet justitiële en strafvorderlijke gegevens (Wjsg) en het bijbehorende besluit.

Voorafgaand aan de inwerkingtreding van de AVG is het Bureau Raad het Project AVG gestart om de overgang naar de AVG te structureren en te borgen. Na de inwerkingtreding van de AVG is het project gestopt. De werkzaamheden zouden in de lijn verder worden opgepakt.

Doel

Om inzicht te behouden in de nog openstaande punten, is het borgingsplan privacy opgesteld. Hierin staat welke activiteiten nog moeten worden ondernomen om in lijn met de privacywetgeving te handelen en het handelen als zodanig te borgen.

Herijking

Om aan het doel van het borgingsplan te volbrengen, wordt het plan minimaal halfjaarlijks herijkt. Hierdoor blijft het borgingsplan een actueel beeld geven van de werkzaamheden die ten aanzien van privacy nog moeten worden verricht. Daarbij wordt ook zo goed als mogelijk inzage gegeven in de planning per werkzaamheid.

Nadat het eerste borgingsplan in januari 2019 is vastgesteld, is het nu onderhavige document de zesde versie.

Leeswijzer

Het vervolg van het document is als volgt. In hoofdstuk 2 wordt een algemeen beeld gegeven over de implementatie en borging van de privacywet- en regelgeving binnen de Rechtspraak. In hoofdstuk 3 wordt ingegaan op hoe en door wie het borgingsplan wordt samengesteld. Vervolgens wordt in hoofdstuk 4 tot en met 7 op basis van de vier privacy management KPI’s van JenV de status ten aanzien van privacy weergegeven. Tot slot worden in hoofdstuk 8 nog enkele onderwerpen behandeld die relevant zijn voor de Rechtspraak, maar niet passen in een van de KPI’s.

2. Beeld Rechtspraak

Er is al veel werk verzet, maar er is ook nog genoeg te doen. Om het algemeen beeld van de Rechtspraak uit te drukken wordt gebruik gemaakt van de termen: ‘in-control’ en ‘compliant’. Met dit eerste wordt bedoeld dat nog niet op alle onderdelen aan de geldende privacywet- en regelgeving wordt voldaan, maar dat wel duidelijk is wanneer hieraan voldaan wordt. Met dit tweede wordt bedoeld dat alle aan onderdelen van de privacywet- en regelgeving wordt voldaan en dat de onderdelen zijn geborgd. Hierbij moet de kanttekening gemaakt worden dat nooit sprake kan zijn van 100% compliancy. De stand van de techniek en de interne en externe omgeving veranderen dusdanig snel dat altijd ruimte is voor verbetering. Borgen volgens de PDCA-cyclus staat daarom centraal.

De Rechtspraak moet tot de conclusie komen dat ze niet in-control of compliant is met de geldende privacywet- en regelgeving. Om in-control te zijn zal de Rechtspraak ervoor moeten zorgen dat er zicht is op de volledige informatievoorziening. Daarna moet er een eenduidige planning zijn om de systemen in de informatievoorziening in lijn te brengen met de privacywet- en regelgeving. Bij dit laatste bestaat de mogelijkheid om systemen, na een risicoafweging, niet meer aan te passen, omdat ze op korte termijn zullen worden uitgefaseerd.

Om compliant te worden, zal de Rechtspraak de actiepunten in dit plan moeten borgen.

3. Werkwijze en totstandkoming

Dit plan is ingedeeld conform de privacy management KPI's vanuit het ministerie van Justitie en Veiligheid (JenV). KPI worden verschillende aandachtspunten behandeld. Deze scoring vindt plaats op twee niveaus: het kwaliteitsniveau en het ambitieniveau. De scoringsniveau's gaan van 1 (laagst) t/m 5 (hoogst). De omschrijving van iedere KPI staat in bijlage 1; de betekenissen van iedere score staat in bijlage 2.

Kwaliteitsniveau
Ieder aandachtspunt krijgt een score voor het kwaliteitsniveau dat past bij de huidige situatie. De score wordt onderbouwd aan de hand van voorbeelden (zoals bestaande afspraken, procedures, processen, diensten en producten). Hieruit moet de passendheid van het aangegeven kwaliteitsniveau blijken.

Ambitieniveau
In relatie tot het kwaliteitsniveau wordt aangegeven wat bij ieder aandachtspunt de ambitie van de Rechtspraak is. Hierbij wordt aangegeven welke acties nodig zijn om tot dat niveau te komen. Aan iedere actie wordt een actiehouder en een deadline gekoppeld, zodat periodiek de voortgang wordt vastgesteld. Tegelijkertijd zorgt een actie ervoor dat privacy wederom aandacht en prioriteit krijgt.

Overall-aanpak
Dit borgingsplan is opgesteld in opdracht van de Raad voor de rechtspraak. Opdrachtnemer is de directeur van het Bureau van de Raad voor de rechtspraak.

De uitvoering van de activiteiten wordt gecoördineerd door een werkgroep met daarin de volgende deelnemers:

- Functionaris gegevensbescherming
- Privacy officer IVO
- Functionarissen privacy IVO
- Teamleider security, privacy & kwaliteit IVO en Wnd CISO
- Hoofd CIO Office
- Beleidsmedewerker privacy bureau Rvdr
- (senior)adviseurs Recht & ICT afdeling Strategie Bureau Rvdr

Agendalid: stafmedewerker Europees recht Landelijk Bureau Vakinhoud rechtspraak

De daadwerkelijke uitvoering van de activiteiten ligt bij een veel grotere groep medewerkers waarbij medewerkers op het terrein van informatiebeveiliging, service delivery, architectuur, applicatiebeheer, inkoop, portefeuillehouders en de lokale privacycoördinatoren bij de gerechten belangrijke partijen zijn.

Beperkingen
Het plan gaat niet in op de activiteiten die door het Landelijk Bureau Vakinhoud rechtspraak (LBVr) worden verricht, waarbij het gaat om de werkzaamheden die liggen in het verlengde van het werk van de rechter. Hiervoor is de werkgroep AVG vakinhoud opgericht die bestaat uit experts vanuit de gerechten. Vanzelfsprekend is er wel samenwerking met en uitwisseling van kennis tussen het LBVr en de betrokkenen vanuit (de bedrijfsvoering van) de Rechtspraak.

Disclaimer
De pilot van JenV die in het bovenstaande kader werd genoemd, wordt door de Rechtspraak gebruikt om te bepalen of deze werkwijze voor de Rechtspraak werkbaar is. Er is dan ook nog geen bestuurlijke goedkeuring gegeven op de genoemde scores. Nadat de pilotfase is afgerond en door JenV formeel goedkeuring is gegeven op de KPI's, zal bestuurlijke vastlegging plaatsvinden van de kwaliteits- en ambitieniveaus.

4. Privacy administratie

De Privacy Administratie omvat alle aandachtsgebieden voor de Rechtspraak die een rol spelen bij het kunnen aantonen van en verantwoorden over de naleving c.q. het compliant werken aan van privacy wet- en regelgeving (Verantwoordingsplicht).

De KPI Privacy Administratie geeft de verwerkingsverantwoordelijke inzicht in de status quo van de wettelijk verplichte documentatieopbouw voor deze aandachtsgebieden (Documentatieplicht) en laat naar buiten zien wat er zoal op de rit is als onderbouwing voor de door de organisatie gehanteerde zorgvuldigheid in haar omgangsvormen met persoonsgegevens.

De KPI Privacy Administratie bestaat uit **zes** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

1 **Register van verwerkingsactiviteiten:** Hierin ligt de onderbouwing van de rechtmatigheid van verwerkingen vast.	
Onderbouwing kwaliteitsniveau:	Het register van verwerkingsactiviteiten geeft in een overzicht een integraal beeld van alle verwerkingen door een (of meerdere) verwerkingsverantwoordelijken. Per verwerking wordt aangegeven wat het doel is, welke (wettelijke) grondslag van toepassing is, hoe lang de persoonsgegevens worden bewaard, etc. Voorafgaand aan de inwerkingtreding van de AVG is door de projectleiding van het AVG-project van het Bureau Rvdr een landelijk verwerkingenregister opgesteld. Het landelijk register bevat de gemeenschappelijke gegevensverwerking door de Rechtspraak. Daarnaast heeft ieder gerecht onder eigen verantwoordelijkheid een lokaal register waarin de verwerkingen staan die naast de Rechtspraakbrede verwerkingen plaatsvinden. In dat kader is gerealiseerd in samenwerking met IVO, gerechten en diensten: ✓ Landelijk register: IT-applicaties (beheer IVO); ✓ Lokale registers: lokale IT en registraties (beheer gerechten en landelijke diensten zelf). Een samenvatting is te vinden via: register van verwerkingen Deze registers waren 25 mei 2018 (nagenoeg) afgerond. Er zijn destijds landelijke applicaties buiten beschouwing gelaten. Deze worden momenteel toegevoegd aan het landelijke register. De Rvdr is als verwerkingsverantwoordelijke verantwoordelijk voor het vullen van het landelijke register. Het bijhouden en verder vullen omtrent de verwerkingen die landelijk plaatsvinden is echter door de Rvdr gedelegeerd aan de privacy officer van IVO. **Landelijk register** Het landelijk register van verwerkingen moet nog worden aangevuld met de landelijke applicaties die buiten beschouwing zijn gelaten. Daarna moet deze worden bijgehouden. **Lokale registers** Er is een inventarisatie geweest van de lokale registers door de beleidsmedewerker privacy van het bureau Rvdr om te onderzoeken in hoeverre de lokale registers voldoen aan de geldende privacywetgeving. Hiervoor is de nieuwe KCD-module worden gebruikt. De meeste gerechten en diensten hebben een eerste stap gezet met het register van verwerkingsactiviteiten. Sommige zijn volledig en voorzien in alle vereisten uit de AVG. De meeste registers gaan nu echter alleen in op de lokale verwerking

	en de persoonsgegevens die daarvoor verwerkt worden. Ze missen de bewaartermijnen, grondslagen, doeleinden en een beschrijving van betrokkenen. De gerechten en diensten zijn via de BVC'ers hierop geattendeerd. Kwaliteitsniveau: gezien het bovenstaande is score 1 het meest passend bij de huidige situatie.
Ambitieniveau:	**Borging en vervolgstap** De Rechtspraak moet ervoor zorgen dat alle lokale en landelijke verwerkingen zijn geïnventariseerd en worden bijgehouden. Hierna kan de vervolgstap gemaakt worden dat overbodige verwerkingen worden beëindigd. De verwachting is dat dit grotendeels gebeurt na de inventarisatiefase. Verwerkingen zullen conform hetgeen in het register staat, moeten gaan plaatsvinden. **Beperking** Volgens de privacy governance is ieder gerecht en iedere dienst zelf verwerkingsverantwoordelijk. Een centraal register van verwerkingen met daarin alle verwerkingen van alle gerechten past niet binnen dit uitgangspunt. Ambitieniveau: gezien het bovenstaande is niveau 2 het beoogde kwaliteitsniveau. Hiervoor moet de volgende acties worden uitgevoerd: • Bijhouden landelijk register (privacy officer IVO; eind Q1 2021) • In het tweede kwartaal van 2021 zal de beleidsmedewerker privacy nagaan of de voorgestelde verbeteringen in de lokale registers zijn doorgevoerd (actie beleidsmedewerker privacy; 2e kwartaal 2021). • Gerechten moeten conform het register van verwerkingsactiviteiten gaan handelen. Dit betekent data tijdig vernietigen en autorisaties beperken tot degenen die bij de verwerking genoemd staan. Zij worden hier door de FG op gewezen.
2 **DPIA's:** hiermee wordt gemonitord dat de risico-inschattingen van verwerkingen aanwezigheid is en kwalitatief adequaat zijn. Dit geeft de verwerkingsverantwoordelijke inzicht in de risico's en zorgt ervoor dat de risico's worden teruggebracht naar een voor de verwerkingsverantwoordelijke acceptabel niveau.	
Onderbouwing kwaliteitsniveau:	De status van dit aandachtspunt wordt uitgesplitst naar de situatie bij: 1) IVO Rechtspraak; 2) het LDCR; en 3) de gerechten en overige diensten. 4) alle Rechtspraakonderdelen Hierbij kan opgemerkt worden dat PIA's plaatsvinden conform het Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA). Daarnaast wordt in sommige gevallen gebruik gemaakt van de PIA Light. **1. IVO Rechtspraak** De Rechtspraak maakt gebruik van een mix van oudere en nieuwe systemen. Deze systemen worden door IVO Rechtspraak beheerd. Van de oude systemen is in het verleden vaak geen PIA uitgevoerd en de PIA's die wel zijn uitgevoerd, zijn veelal niet meer actueel. Deze PIA's worden met terugwerkende kracht alsnog opgesteld. Voor nagenoeg alle primaire processystemen is in 2019 en 2020 een PIA opgesteld. Om nieuwe omissies te voorkomen wordt sinds 2016 elk nieuw (te ontwikkelen) systeem onderworpen aan een PIA. Bij aanpassingen wordt de bestaande PIA herijkt.

Om het proces voor het uitvoeren van PIA's te borgen is door IVO een procesbeschrijving opgesteld. De procesbeschrijving gaat in op het uitvoeren van PIA's voor nieuwe projecten, bestaande diensten en de periodieke herijking van PIA's.

2. LDCR

Het LDCR verzorgt onder andere de inkoop van producten en diensten voor gerechten. Voor het overgrote deel van de verwerkingen die worden ingekocht, worden in meer of mindere mate persoonsgegevens verwerkt. Deze verwerkingen moeten conform de privacywet- en regelgeving plaatsvinden. Dit betekent dat met terugwerkende kracht moet worden gecontroleerd dat voor iedere afgenomen dienst een PIA is uitgevoerd en een verwerkersovereenkomst (indien nodig) is afgesloten.

Sinds de inwerkingtreding van de privacywet- en regelgeving is door het LDCR een werkproces opgesteld voor verplichtingen uit deze wet- en regelgeving in het de aankoop- en aanbestedingstrajecten. Verder heeft LDCR/Inkoop een inhaalslag gemaakt om qua PIA's en verwerkersovereenkomsten aan de AVG-verplichtingen te voldoen. Er is nog een overeenkomst waarbij voldaan moet worden aan de AVG-verplichten.

Voor alle andere landelijke contracten is bepaald of er een PIA moet plaatsvinden en/of een verwerkersovereenkomst moet worden opgesteld. Bij nieuwe overeenkomsten wordt gecontroleerd of een PIA gedaan is en of een verwerkersovereenkomst moet worden opgesteld. Naar aanleiding van een cursus

3. Gerechten en overige diensten

Ieder gerecht heeft een register van lokale verwerkingsactiviteiten (zie hiervoor). Aan iedere verwerking in het register moet een PIA ten grondslag liggen waaruit de informatie voor het register blijkt. Denk aan het doel van de verwerking, de bewaartermijn en de ondersteunende systemen.

Ter controle van dit proces is in april 2020 via het Key Control Dashboard (KCD) uitgevraagd in hoeverre de nodige lokale PIA's zijn uitgevoerd. Uit de uitvraag is gebleken dat PIA's nog onvoldoende plaatsvinden vanwege een gebrek aan kennis. Daarom is eind september 2020 een cursus gegeven aan de privacycoördinatoren om de benodigde kennis bij te brengen. Begin 2021 vindt een vervolgcursus plaats.

Ondanks dat bij de gerechten PIA's onvoldoende plaatsvinden, wordt het overgrote deel van de verwerkingen afdekt met PIA's die door IVO en/of het LDCR worden uitgevoerd of gesignaleerd. Indien wordt gesignaleerd dat een PIA nog moet worden uitgevoerd, wordt dit aangegeven bij het betreffende gerecht.

4. Alle Rechtspraakonderdelen

Als de PIA eenmaal is uitgevoerd, is het volgens de PDCA-cyclus van belang dat op de bevindingen wordt geacteerd. Acteren betekent: accepteren of mitigeren. In geval van accepteren geldt voor risico's met een hoge score dat ze, voorafgaand aan de acceptatie, ter advisering worden voorgelegd aan de toezichthouder. In de praktijk wordt hiervoor de wettelijke procedure gebruikt. IVO voegt dit toe aan de procesbeschrijving AVG.

	Kwaliteitsniveau: op basis van het bovenstaande is niveau 2 het meest passend.
Ambitieniveau:	Ten aanzien van de PIA vindt nog onvoldoende plaats: - uitvoering door de gerechten; - monitoren van de voortgang van de acceptatie of mitigatie van risico's; - herzien van de PIA's, waardoor het cyclische karakter van privacy-risicomanagement ontbreekt. **Implementatie PIA-tool** In 2021 wil de Rechtspraak gebruik gaan maken van een PIA tool. Deze tool zal: - het PIA-proces versnellen door het automatiseren; - de kwaliteit verbeteren doordat de tool de gebruiker kennis aanreikt; - signaleren als een PIA na een bepaalde periode moet worden herijkt; - automatisch het register van verwerkingsactiviteiten bijwerken. Door de directeur van IVO is goedkeuring gegeven om de software voor het maken van PIA's te gaan aanbesteden. De implementatie van deze tool is aanvankelijk gestagneerd op nieuwe mantelovereenkomst. Verdere stagnatie werd vervolgens veroorzaakt doordat de tool door de cloud regiegroep van IVO moet worden goedgekeurd. In februari 2021 wordt SmartPIA in de cloud regiegroep van IVO besproken. Ambitieniveau: de Rechtspraak beoogt niveau 3 te behalen. Hiervoor moeten de volgende acties worden uitgevoerd: • Updaten procesbeschrijving AVG (Privacy officer, 1e kwartaal 2021) • Implementatie PIA-tool (IVO, 2e kwartaal 2021)
3 **Toestemmingsregister:** binnen dit aandachtspunt gaat het over de aanwezigheid en kwaliteit van registraties waaruit de omgang met toestemming voor het verwerken van persoonsgegevens (en het weer kunnen intrekken daarvan) blijkt.	
Onderbouwing kwaliteitsniveau:	**De rol van toestemming voor de Rechtspraak** Toestemming in de zin van de AVG heeft voor de Rechtspraak, vergeleken met andere organisaties, in het primaire proces een beperkte rol. De verwerkingen van de Rechtspraak worden namelijk grotendeels gebaseerd op de grondslagen: - wettelijke verplichting (art. 6, lid 1, sub c AVG); en - de taak van algemeen belang (art. 6, lid 1 sub e AVG). Bij innovatieve projecten of in de bedrijfsvoering heeft toestemming als grondslag een iets grotere rol. **Documentatie van toestemming** Dit onderdeel is tweeledig. Enerzijds moet toestemming als grondslag in het register van verwerkingsactiviteiten bij een verwerking worden opgenomen. Anderzijds is het van belang dat de Rechtspraak de verkregen toestemmingen bewaard. Volgens de privacywet- en regelgeving is het verplicht om de toestemming (en de intrekking daarvan) te documenteren. Ieder gerecht en elke dienst is hiervoor zelf verantwoordelijk. Vanuit het Bureau Rvdr wordt hier niet op toegezien, omdat ieder gerecht zelf verantwoordelijk om de grondslag te borgen. Vanuit het Bureau Rvdr wordt advies verleend indien nodig. Kwaliteitsniveau: gezien het bovenstaande is de score 2.

Ambitieniveau:	Voor de Rechtspraak is het van belang dat voor ieder gerecht en voor iedere landelijke dienst te allen tijde duidelijk is bij welke verwerkingen de grondslag toestemming wordt gebruikt en dat het proces hieromtrent vastgelegd en geborgd is. Door de FG wordt hierop toegezien. Via het KCD zal dit worden uitgevraagd. Of sprake is van de grondslag toestemming zal onder andere moeten blijken uit de lokale registers van verwerkingsactiviteiten. <u>Ambitieniveau:</u> gezien het bovenstaande streeft de Rechtspraak naar niveau 3. Actie: • Via het KCD wordt bij de gerechten en diensten uitgevraagd in hoeverre wordt voldaan aan de wettelijke plicht om toestemming (en de intrekking daarvan) te registreren (beleidsmedewerker privacy, 2e kwartaal 2021).
4 **Datalekregister:** de wijze waarop informatiebeveiligingsincidenten worden gedocumenteerd, beheerd en qua afhandeling (waaronder de kwalificatie datalek toekenning) worden bewaakt	
Onderbouwing kwaliteitsniveau:	Sinds de zomer van 2016 is er een procedure voor het melden van datalekken. In oktober 2019 is deze procedure vernieuwd in het handboek datalekken. De beveiligings- en privacycoördinatoren bij gerechten en diensten zijn verantwoordelijk voor de uitvoering van de procedure. Het registeren gebeurt op dit moment nog met behulp van het softwarepakket Classbase. Op het initiatief van het LOBRO is er een sharepointsysteem ontwikkeld waarmee de registratie van datalekmeldingen geüniformeerd is. Dit systeem heeft als voordeel dat eventuele meldingen naar de toezichthouder direct gegenereerd kunnen worden. Met de Hoge Raad zijn afspraken gemaakt dat het formulier uit dit systeem door hen wordt geaccepteerd. De FG en de BVA zorgen, met hulp van de Medewerker BVA, voor overzichten ten behoeve van de viermaandsrapportage en het jaarverslag. Deze rapportages worden gedeeld met het LOBRO en het SBO, zodat zij kunnen kennisnemen van de resultaten en de daarop gebaseerde adviezen. Veel van de datalekken hangen samen met het onvoldoende anonimiseren van uitspraken die gepubliceerd worden of met het verkeerd versturen van documenten. Door de Medewerker BVA wordt onderzocht op welke manier de meest voorkomende datalekken kunnen worden verminderd. <u>Kwaliteitsniveau</u>: gezien het bovenstaande bevindt de Rechtspraak zich op dit moment op niveau 4.
Ambitieniveau:	Het landelijk overleg van BVC'ers, het LOBRO, heeft een inventarisatie gedaan waaruit blijkt hoe er bij de gerechten omgegaan wordt met verwerking, registratie en meldingen van datalekken. Uit de cijfers over meldingen blijkt een verschil in aanpak per gerecht. Om te komen tot een uniforme werking is het sharepointsysteem ontwikkeld. Er is echter nog een verschil in de gevallen waarin melding wordt gedaan bij de toezichthouder. Het ene gerecht meldt alles en sommige gerechten uitsluitend 'ernstige' datalekken. Dit zal door het (DB) LOBRO met de PGHR worden besproken. <u>Ambitieniveau</u>: de Rechtspraak beoogt haar huidige kwaliteitsniveau te handhaven en te verbeteren, doch niet per se tot niveau 5. Acties:

	• Afspraken uniforme melding datalekken (LOBRO; eind 4e kwartaal 2021) • Uitvragen anonimiseringstool (IVO; 4e kwartaal 2020)
5 Gegevensbeschermingsbeleid Hiermee wordt het voor iedereen binnen de organisatie duidelijk hoe met persoonsgegevens wordt omgegaan.	

Onderbouwing kwaliteitsniveau:	Het privacybeleid wordt in meerdere documenten op meerdere niveaus vormgegeven:
	- Strategisch niveau:
	  o Strategisch plan privacy
	  o Beveiligingsbeleid voor de Rechtspraak 2019-2023
	- Tactisch niveau:
	  o Minimumnormen beveiliging en privacy
	  o IT-normenkader
	  o Intern beleid (bijv. Privacybeleid IVO)
	- Operationeel niveau:
	  o Procesbeschrijvingen en best practices
	
	Het beleid wordt periodiek herijkt op basis van de PDCA-cyclus.
	Hieronder wordt nader ingegaan op de implementatie van de BIO en de verwerking van persoonsgegevens door HRM, inkoop en externe onderzoeken.
	
	BIO
	Nadat IVO Rechtspraak in januari 2020 is overgestapt op de BIO, hebben de gerechten en andere diensten ook besloten over te stappen naar de BIO.
	
	Om de gerechten en diensten bij de overgang naar de BIO te ondersteunen, wordt door het Bureau BVA in kaart gebracht welke minimumnormen moeten worden aangepast aan de BIO te voldoen. Hierbij wordt ook gekeken op welke manier ze gerechten moeten worden gefaciliteerd. Deze inventarisatie wordt afgestemd met het LOBRO en IVO.
	
	Verder wordt door IVO geïnventariseerd wat zij aan IT-securitybeleid moeten aanpassen om het beleid in lijn te brengen met de BIO. Momenteel wordt een nulmeting uitgevoerd op de dienst om te zien waar de hiaten zitten. Verder wordt de PDCA-cyclus ingericht om in control te komen en te blijven. De BIO wordt per hoofdstuk vertaald naar handreikingen (intern beleid). Logging is daarbij als eerste opgepakt. Er worden sessies gegeven om de BIO kennis op niveau te brengen.
	
	Uitdragen van beleid
	Tegelijkertijd wordt het (informatiebeveiligings)beleid actief uitgedragen door het management, maar blijft het nog achterwege voor wat betreft privacy. Ook aan privacyopleidingen wordt nog onvoldoende gedaan.
	
	Verwerking van personeelsgegevens
	Door de HRM-afdelingen, Inkoop en externe onderzoekers binnen de Rechtspraak worden veel (vertrouwelijke) persoonsgegevens verwerkt. Het is van belang dat deze gegevens rechtmatig worden verzameld, rechtmatig worden verwerkt en tijdig worden verwijderd.
	
	Naar aanleiding van signalen dat persoonsgegevens onveilig worden verstuurd, is het van belang om hier extra aandacht aan te besteden.
	
	Kwaliteitsniveau: op basis van het bovenstaande is 3 het best passende niveau.

Ambitieniveau	Ambitieniveau: niveau 5 is haalbaar voor de Rechtspraak en moet ook de ambitie zijn. Beleid wordt opgesteld, door het bestuur vastgesteld en periodiek herijkt op basis van de PDCA-cyclus. Verbeteringen zijn gelegen in: - het meer actief uitdragen van het privacybeleid door de besturen en directies en het faciliteren van opleidingen; en - verbeter van de procedures en gegevensverwerking in het kader van HRM, inkoop en onderzoeken. Acties: - Faciliteren van de overstap naar de BIO voor de gerechten (beleidsmedewerker privacy; 1e kwartaal 2022). - Met de afdelingen HRM, Inkoop en externe onderzoek in gesprek om ervoor te zorgen dat privacy ook bij deze disciplines goed geborgd worden (FG/Adviseur privacy & informatiebeveiliging; 2e kwartaal 2021)
6 Privacyverklaring Met een privacyverklaring wordt de informatieplicht over het verwerken van informatie door de verwerkingsverantwoordelijke naar betrokkenen vormgegeven.	
Onderbouwing kwaliteitsniveau:	Door de Rechtspraak is de algemene privacyverklaring gepubliceerd op rechtspraak.nl. De informatie hierin is uitgesplitst per rechtsgebied. Daarnaast is onlangs op de vacaturepagina van de Rechtspraak een aparte privacyverklaring gepubliceerd. Kwaliteitsniveau: op basis van het bovenstaande is niveau 2 het best passend.
Ambitieniveau:	Het ambitieniveau is 3. Hiervoor moet de Rechtspraak meer grip krijgen op gegevensverwerkingen die naast het primaire proces plaatsvinden, zoals het wervings- en selectietraject. Hierna kan de informatieplicht hierop worden aangepast. De realisatiedatum van deze ambitie is afhankelijk van de samenwerking met o.a. teams HRM, Inkoop en externe onderzoeken. Verder is dit ambitieniveau ook afhankelijk van het werk bij de gerechten. Uiteindelijk zal volgens een cyclisch proces de privacyverklaring worden bijgewerkt. Gezien de datum van de actie in het vorige ambitieniveau, kan een eerste aanpassing verwacht worden in het 2e of 3e kwartaal 2021. Een definitieve einddatum kan niet worden gegeven.

5. Transparantie

De KPI Transparantie geeft aan op welke wijze de verwerkingsverantwoordelijke namens diens organisatie invulling geeft aan het transparantiebeginstel, dat onderdeel uitmaakt van de Rechten van Betrokkenen. Transparantie is een onderdeel van de informatieplicht die op de verwerkingsverantwoordelijke rust en gaat over gepaste openheid over de gehanteerde zorgvuldigheid bij het verwerken van persoonsgegevens.

De wijze van informatieverstrekking wordt situationeel bepaald en is een belangenafweging. Dit kan persoonlijk en al dan niet 'just-in-time' (mondeling, brief, aanreiken van flyer, digitaal/internet) of indirect en meer algemeen via een privacyverklaring worden vormgegeven, waarbij vereiste informatie voor betrokkenen op of vanuit één plek vindbaar is dan wel wordt aangeboden. Dit informeren gaat in principe altijd vóóraf aan het verwerken van persoonsgegevens van betrokkenen door of namens de verwerkingsverantwoordelijke. Dat dit heeft plaatsgevonden is aantoonbaar.

De KPI Transparantie bestaat uit **drie** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

1 **Inhoud informatie:** dit omvat **wat** wordt vastgelegd (instroom) en **waarom**, **wie** er toegang heeft tot deze informatie en/of aan wie en waarom worden welke persoonsgegevens verstrekt (doorstroom) maar ook het aangeven hoe lang persoonsgegevens worden bewaard en **wanneer** en op **welke** wijze deze persoonsgegevens weer worden verwijderd, vernietigd en/of gearchiveerd (uitstroom).	
Onderbouwing kwaliteitsniveau:	Bij dit aandachtspunt gaat het over de informatie die onder andere in de privacyverklaring is opgenomen. Op rechtspraak.nl/privacy worden de 5w- en h- vragen beantwoord onder de veel gestelde vragen. Verder gelden voor de bewaartermijnen van documenten in het primaire proces de basisselectiedocumenten. Deze zijn gepubliceerd op nationaalarchief.nl Gezien het bovenstaande voldoende de Rechtspraak aan kwaliteitsniveau 3.
Ambitieniveau:	Met de aanschaf van de PIA-tool ontstaat een meer structureel proces om privacy te borgen. Dit zal er ook voor zorgen dat de gepubliceerde informatie op basis van de PDCA-cyclus steeds zal worden bijgewerkt. Op dit moment heeft de Rechtspraak ambitieniveau 4.
2 **Toegankelijkheid informatie:** dit omvat het tijdig, begrijpelijk en gemakkelijk, in duidelijke en eenvoudige taal verstrekken dan wel ontsluiten of beschikbaar maken van relevante informatie over verwerkingen van persoonsgegevens aan betrokkenen of belanghebbenden.	
Onderbouwing kwaliteitsniveau:	Voor rechtszoekenden en professionals moet het eenvoudig zijn om informatie te vinden over de wijze waarop de Rechtspraak omgaat met persoonsgegevens. Uit aandachtspunt 6 van de KPI Privacy Administratie is gebleken dat de Rechtspraak op twee verschillende plekken een privacyverklaring heeft gepubliceerd: - een algemene op rechtspraak.nl; en - een verklaring die aansluit bij de sollicitatieprocedure van de Rechtspraak. Mochten betrokkenen geïnteresseerd zijn in meer informatie over de Rechtspraak dan kunnen ze gebruikmaken van de verschillende communicatiekanalen die de Rechtspraak aanbiedt, zoals Facebook, Twitter, Instagram en Whatsapp. Kwaliteitsniveau: gezien het bovenstaande ligt niveau 3 het meest in de rede.

Ambitieniveau:	Net als bij het vorige aandachtspunt zal de privacyverklaring door de nieuwe PIA-tooling continu worden geüpdatet. Verder kunnen ook vragen van betrokkenen aanleiding geven om de gepubliceerde informatie aan te passen. Het ambitieniveau is 4.
3 Faciliteren uitoefenen privacy rechten door betrokkenen Transparantie gaat over de eenvoud waarop betrokkenen gebruik kunnen maken van hun privacy rechten	
Onderbouwing kwaliteitsniveau:	De privacywet- en regelgeving bieden rechtszoekenden en professionals de mogelijkheid om bepaalde rechten uit te oefenen. Het gaat dan bijvoorbeeld om recht op inzage, het recht van rectificatie en het recht om vergeten te worden. Om deze rechten te faciliteren is op rechtspraak.nl/privacy een procedure gepubliceerd hoe betrokkenen van hun rechten gebruik kunnen maken. Voor interne betrokkenen is het een en andere gepubliceerd op Intro. De procedures zijn ingevoerd binnen de Rechtspraak. Tijdens de implementatie is het volgende gerealiseerd: • Procedurebeschrijvingen en modelbrieven zijn aan gerechten en diensten ter beschikking gesteld door het AVG-projectteam van het Bureau Raad; • Gerechten en diensten zijn geïnformeerd over de procedure tijdens een aparte themamiddag; • Gerechten hebben een eigen coördinator informatieverzoeken die bereikbaar is Bij inwerkingtreding van de AVG werden de gerechten en diensten door de landelijk coördinator informatieverzoeken ondersteund bij het afhandelen van privacyverzoeken van betrokkenen. Al snel bleek dat de gerechten in staat waren de vragen zelf af te handelen. Vanwege een gebrek aan meerwaarde is de rol nu niet meer ingevuld. Eventuele vragen kunnen gerechten altijd stellen via [redacted]@rechtspraak.nl. Kwaliteitsniveau: op basis van het bovenstaande en de indicatoren is 5 het meest passende niveau.
Ambitieniveau:	Er zijn geen signalen dat er op dit punt op korte termijn nog acties ondernomen dienen te worden.

6. Privacy by design (PbD) en Default

Met Privacy by design wordt inzicht gegeven in de mate waarin rekening wordt gehouden met het kwaliteitsaspect privacy als aandachtspunt bij het ontwikkelen van nieuwe (werk)processen, informatiesystemen en/of beleid of wetgeving. Met privacy by default wordt beoogd (werk)processen, informatiesystemen en/of beleid te leveren die standaard uitgaan van de minst inbreukmakende gegevensverwerking.

De focus van de KPI PbD ligt daarmee bij het borgen van de belangenbescherming van de betrokkene waar persoonsgegevens van worden verwerkt.

De KPI Privacy by design en privacy by default bestaat uit **drie** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

<table>
<tr><td colspan="2">1 Privacy wordt meegenomen in ontwerpfase: PbD omvat het vroegtijdig bij en gedurende de doorlooptijd van nieuwe ontwikkelingen aandacht schenken aan de privacy aandachtsgebieden</td></tr>
<tr><td>Onderbouwing kwaliteitsniveau:</td><td>Ten aanzien van privacy in de ontwerpfase is een onderscheid te maken tussen:
- ontwikkelingen bij IVO;
- ontwikkelingen bij gerechten en andere diensten.

IVO
De meeste IT-ontwikkelingen vinden plaats bij IVO Rechtspraak. Voor zover er lokale ontwikkelingen zijn, zal privacy ad hoc aandacht krijgen in de ontwerpfase.

Tegelijkertijd wordt bij IVO privacy by design geïmplementeerd in de ontwikkelprocedures. Bij steeds meer ontwikkelingen wordt privacy by design gebruikt, maar een structurele aanpakt waarbij privacy daadwerkelijk vanaf het begin betrokken is, is nog in ontwikkeling. Hiervoor wordt samengewerkt met de ontwikkelteams. Met terugwerkende kracht worden ook de oude IT-systemen AVG-compliant gemaakt (hierover meer onder aandachtspunt 2 van deze KPI).

Andere gerechten en diensten
Het principe van PbD is bij de gerechten onvoldoende bekend. Desalniettemin betekent dit niet dat er (grote) steken vallen. Diensten en IT-producten worden via de inkoopafdeling van het LDCR of IVO aangeschaft. Bij deze inkoopafdelingen zijn procedures ontwikkeld om privacy te borgen door een PIA uit te voeren en, voor zover nodig, door verwerkersovereenkomsten af te sluiten. Hierdoor wordt bij het aanbesteden van een nieuwe lokale dienst of ontwikkeling de privacy toch op een vroeg stadium in de aanschaf meegenomen. Enkel bij lokale initiatieven zal privacy onvoldoende meegenomen worden.

<u>Kwaliteitsniveau:</u> gezien het bovenstaande is niveau 2 het best passend.</td></tr>
<tr><td>Ambitieniveau:</td><td>De gerechten en de landelijke diensten moeten nog groeien in het toepassen van privacy by design. Er zijn ontwikkelingen, maar deze zorgen er nog niet voor dat privacy vanaf het begin al in scope is. Verder ontbreekt nog een cyclische werkwijze waarbij:
1) privacyrisico's vanaf dag één in kaart worden gebracht,
2) de maatregelen ter mitigatie van de risico's tijdens de ontwikkeling worden geïmplementeerd,</td></tr>
</table>

	3) de maatregelen in het register van verwerkingsactiviteiten worden opgenomen en 4) periodiek wordt op de effectiviteit van de maatregelen gecontroleerd. Dit laatste kan leiden tot eventuele aanpassingen. Ambitieniveau: het ambitieniveau is 3. Hiervoor moeten de volgende acties worden ontplooid: - Verder implementeren van privacy by design bij IVO Rechtspraak door o.a. het uitvoeren van PIA's (IVO) - Voorts zullen de gerechten ondersteund worden in de toepassing van privacy by design bij lokale initiatieven waarbij persoonsgegevens worden verwerkt (beleidsmedewerker privacy, 2e kwartaal 2021).
2 Afwegingen in het kader van beoordeling passende maatregelen PbD betekent het bij ontwikkelingstrajecten gestructureerd aandacht geven aan de beoordeling van wat passend is bij de aard, omvang, context en doel van de verwerking en ook anderszins proportioneel is (bijvoorbeeld kostentechnisch) dan wel subsidiair (kan het verwerken ook op een andere wijze, met minder risico's voor betrokkenen).	
Onderbouwing kwaliteitsniveau:	Artikel 32 van de AVG bepaalt dat persoonsgegevens op een passende manier moeten worden beveiligd. Dit betekent dat rekening moet worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. **Algemeen oordeel** Kwaliteitsniveau: op dit moment is niveau 2 het meest passend bij de status van de Rechtspraak. Bij het merendeel van de verwerkingen zijn de maatregelen in kaart gebracht en geïmplementeerd. Er is echter nog werk dat opgepakt en gestructureerd moet worden uitgevoerd. Ter bespreking hiervan wordt een onderscheid gemaakt in: rubricering, bewaartermijnen, het wegwerken van auditbevindingen, het project AVG en autorisatiebeheer. Uiteindelijk wordt afgesloten met de kwaliteitsscore. **Rubricering** Rubriceren is het labelen van data op basis van de vertrouwelijkheid. Naar aanleiding van de collegiale toets is geconstateerd dat rubricering van datalekgevoelige informatie onvoldoende gebeurt. Om dit probleem op te lossen zijn er drie paden opgezet: - Aan de gerechtsbesturen is geadviseerd dat ze hun verantwoordelijkheid moeten nemen inzake het rubriceren van analoge informatie. - Voor het rubriceren van digitale informatie is in februari 2020 aan het project verzocht om in kaart te brengen wat moet gebeuren om rubriceren van vertrouwelijke en hoog vertrouwelijke data werkbaar te maken. Dit verzoek is echter niet teruggekomen in het faseplan van het project. **Bewaartermijnen** Voor de Rechtspraak zijn de bewaartermijnen vastgelegd in zogenoemde 'Basis Selectie Documenten' (BSD). Deze zijn: - Het BSD Rechtelijke macht (geactualiseerd januari 2021): https://www.nationaalarchief.nl/archiveren/kennisbank/primair-proces-van-de-rechtspraak-selectielijst-voor-de-waardering-van-alle

	- Het BSD Bedrijfsvoering Rechtspraak (inclusief P-dossier): https://zoek.officielebekendmakingen.nl/stcrt-2018-23197.html Door het ministerie zijn nieuwe selectielijsten opgesteld en gepubliceerd. De Rechtspraak zal hierop moeten acteren en zijn eigen selectielijsten aanpassen om in lijn te lopen met het ministerie. Op basis van deze richtlijnen dienen de concrete bewaartermijnen per (onderdeel van een) systeem te worden opgetekend. In principe zijn de basisselectiedocumenten zowel voor papier als voor gegevens opgenomen in digitale systemen. Door de IVO-portefeuillehouder Generieke systemen/Bedrijfsvoering is, in afstemming met medewerkers van het Bureau Rvdr, een advies geformuleerd hoe bewaartermijnen uit de basisselectiedocumenten vertaald zou kunnen worden naar systemen. Op dit moment is het beleid nagenoeg gereed. In eerste instantie was de verwachting dat de beleidslijn in 2020 was afgerond. Door ziekte is het werk echter blijven liggen. De verwachting is dat de beleidslijn in januari 2021 wordt vastgesteld door de stuurgroep. Daarna gaat de beleidslijn door naar het SBO. **Het wegwerken van auditbevindingen** In 2019 heeft de actie gelopen om de auditbevindingen t.a.v. informatie-beveiliging op te schonen. Dit heeft geresulteerd dat in 2019 totaal 195 bevindingen zijn afgesloten. In 2020 zijn vervolgens 142 weggewerkt waardoor er nog 353 bevindingen open staan. Deze risico's zijn onderkend en worden gemonitord. **Het Project AVG** Door IVO is een project gestart waarin systemenanalyses worden uitgevoerd om te bepalen welke aanpassingen gerealiseerd moeten worden om ze in lijn te brengen met de geldende privacywetgeving. Uiteindelijk is het dan aan de dienstenmanagers en portefeuillehouders om de aanpassingen in de systemen door te voeren. • Door het project is een faseplan opgesteld waarin gedetailleerder op de materie per systeemniveau wordt ingegaan. Dit document is op 1 september 2020 geaccordeerd door de stuurgroep van het project. • Voor het aanpassen van de systemen zullen nog een aantal beleidsmatige keuzes moeten worden gemaakt. Dit betreft o.a. t.a.v. bewaartermijnen (zie hierboven) en logging (zie hieronder). Om de maatregelen te kunnen implementeren is door het team architectuur van IVO Rechtspraak een statement opgesteld die in januari 2021 wordt geaccordeerd door de Design Authority van IVO Rechtspraak. Met dit statement is een fundament gelegd voor het ontwerp van o.a. logging. • In het geaccordeerde faseplan is een planning opgenomen voor het aanpassen van (primair proces)systemen. Iedere 6 maanden vindt een actualisatie van de planning plaatst. De eerste actualisatie vindt plaats in maart 2021. In eerste instantie is aangegeven dat de ambitie was om de wijzigingen begin 2022 doorgevoerd te hebben. Die planning was echter niet realistisch, omdat de verantwoordelijkheid voor het realiseren van de maatregelen buiten het project liggen. De deadline is nu 31 december 2022. • De aanpassingen ten aanzien van GPS worden onder leiding van het OM uitgevoerd. Het doel is om deze in maart 2021 te hebben afgerond.

	Logging De Wjsg, AVG en UAVG vereisen logging van gebruikershandelingen door de systemen. Door het ministerie van Justitie en Veiligheid is op 1 januari 2019 een KB gepubliceerd waarmee uitstel is verleend van de loggingsverplichting. Binnen IVO moet het interne loggingsbeleid worden aangepast en vastgesteld mede gelet op de Wjsg. Na vaststelling van het beleid kan verder worden geïmplementeerd in de systemen conform het eerdere plan. Er zal een meerjarig plan worden opgesteld om logging op orde te brengen. **Status aanpassing landelijk beheerde systemen** Begin oktober 2020 hebben de CIO Rechtspraak en de directeur Bureau Rvdr de onhaalbaarheid van de Wjsg-deadline naar de Raad voor de rechtspraak gesignaleerd. Door de CIO wordt bezien wat de precieze problematiek is en welke technische oplossingen er zijn. Ook zal bezien moeten worden wat e.e.a. betekent voor de investeringsplanning. Daarnaast zal bezien moeten worden welke preventieve, flankerende maatregelen genomen kunnen worden via bewustzijnsacties en via stringenter autorisatiebeheer. Het is aan de IVO directie en de onderliggende dienstenmanagers om de landelijk beheerde systemen in lijn met de privacywetgeving te brengen. De business (lees: dienstenmanagers) moet daarvoor een risicoanalyse uitvoeren o.b.v. de minimumnorm risicoanalyse IT. Op basis van de risicoanalyse kan een gewogen besluit genomen worden of een systeem wel of niet wordt aangepast. SP&K IVO heeft hiervoor een afwegingskader opgesteld. Dit afwegingskader ondersteunt bij het maken van een afweging of maatregelen worden doorgevoerd of dat het restrisico wordt geaccepteerd. Op dit moment voldoet Toezicht aan de eisen uit de privacywetgeving. Voor de andere systemen wordt gewerkt aan een risicoafweging om te bepalen of maatregelen worden genomen. Hiervoor is geen planning beschikbaar gesteld. **Autorisatiebeheer** Het autorisatiebeleid is volgens de PwC-accountant niet op orde en de belangrijkste bevindingen waren[1]: • het ontbreken van (uniforme) procedurebeschrijvingen omtrent het toekennen, wijzigen en tijdig ontnemen van rechten in de primaire processystemen; • het ontbreken van inzicht in welke gebruikers over welke toegangsrechten beschikken in de primaire processystemen; • het ontbreken van een periodieke controle op de juistheid van de toegekende rechten aan gebruikers in de primaire processystemen. Om deze punten op te pakken lopen twee projecten: SIMS en informatierotonde. *SIMS* IVO is in 2019 een project gestart waarbij de rechtspraak aansluit op het systeem voor identiteitenmanagement van J&V (SIMS). Het project was begin 2021 al met 4 locaties live. Het bureau Raad wordt als eerstvolgende aangesloten. Volgens planning is de migratie begin april afgerond. *Informatierotonde*

[1] PricewaterhouseCoopers Accountants N.V., Raad voor de rechtspraak Controle 2020 Rapportage interimbevindingen (Management Letter), 7 dec 2020.

	Een andere project dat is opgestart na de bevindingen van de accountant, is het project autorisaties. Dit traject is samen opgepakt met functioneel beheer van IVO (o.a. Leon Sars en Saskia van Batenburg). Om inzicht voor elkaar te krijgen maakt het project gebruik van de informatierotonde, waarmee het mogelijk wordt om diverse gegevensbestanden van samenhang te voorzien en daaruit output te generen. Inmiddels is het project zover dat een groot aantal systemen (bijv. Civiel, Berber, Reis, Nias, Gps, Compas, etc.) in de informatierotonde zijn gekoppeld en dat enkele gerechten zijn voorzien van 'foutenlijsten' waarmee zij aan de slag kunnen. Met de publieke aandacht voor de problemen rondom de autorisaties bij de Politie, het UWV en recent ook de GGD komt ook voor de Rechtspraak de vraag op of dit bij ons wel goed geregeld is. Met het project autorisaties wordt hard gewerkt om hierin inzicht te verkrijgen. Daarna moet worden bepaald wie welke rechten mag hebben en of dit conflicten oplevert. Daarnaast merken de gerechten nu welke meerwaarde de informatierotonde heeft en komen er meermaals verzoeken om nog meer bestanden te koppelen. Na de opzet van een hoedanigheden platform wordt het mogelijk om ook de beveiligingsniveaus van informatie vast te leggen (classificatie of rubricering).
Ambitieniveau:	Zoals uit de bespreking hierboven blijkt, is de Rechtspraak goed op weg om de privacy structureel in de organisatie te borgen. Met de acties bij deze KPI ambieert de Rechtspraak te komen tot kwaliteitsniveau 5. Hiermee sluit zij aan bij de voorbeeldfunctie die de Rechtspraak in de maatschappij heeft. Hier wordt een onderscheid gemaakt in: algemeen, rubricering, bewaartermijnen, het wegwerken van auditbevindingen en autorisatiebeheer. **Algemeen** • Opstellen planning en realiseren aanpassingen systemen (IVO Rechtspraak). **Rubriceren** Acties: • Bij de implementatie van de BIO wordt ook gewerkt aan een nieuw rubriceringskader. Dit rubriceringskader moet na afronding gedeeld worden met de gerechten, zodat zij dit kunnen gaan toepassen (beleidsmedewerker privacy en IVO; 1e kwartaal 2022). **Bewaartermijnen** Acties: • Vaststellen concrete bewaartermijnen voor digitale systemen door Raad (4e kwartaal 2020); • Vertalen naar systemen en processen (IVO en LOV's); • Inregelen mogelijkheden tot automatisch verschonen (IVO + portefeuillehouders). **Het wegwerken van auditbevindingen** Acties: • Audit bevindingen t.a.v. beveiliging krijgen een hogere prioriteit en worden directer gemonitord (IVO, eind 2020). **Autorisatiebeheer**

	Het projecten worden gevolgd door de beleidsmedewerker privacy. De PIA's voor het project zijn voorgelegd aan en positief beoordeeld door de FG.
3 Privacy by default Bij het beschermen van de persoonlijke levenssfeer van de betrokkene voorop staat bij ontwikkelkeuzen. Dit betekent dat altijd die optie wordt geselecteerd die in potentie de minste impact op de persoonlijke levenssfeer van een betrokkene zal hebben.	
Onderbouwing kwaliteitsniveau:	Het privacybewustzijn neemt steeds verder toe en medewerkers stellen steeds vaker vragen waarmee qua privacy rekening gehouden moet worden. Aan de andere kant gebeurt er ook nog veel onder de radar. Het kwaliteitsniveau is: 2. De reden hiervoor is dat er wordt nagedacht over de verwerking met de minst grote impact, maar nog niet structureel. Tegelijkertijd wordt er ook nagedacht over een juiste borging, maar dit moet nog gerealiseerd worden. Hieraan zal de PIA-tool bijdragen.
Ambitieniveau:	Zoals hierboven blijkt is het ambitieniveau minimaal 3. De Rechtspraak beoogt het bewustwordingsniveau verder te vergroten en privacy by default structureel te borgen. De eerste stap is de PIA tool, zodat PIA's eenvoudiger kunnen worden uitgevoerd. Daarna kan het privacyproces verder worden geborgd. Hiervoor is geen concrete termijn te geven, omdat het afhankelijk is van het privacybewustzijn onder medewerkers.

7. Betrokken partijen

De KPI Betrokken partijen geeft inzicht in de wijze waarop organisatiegrens overschrijdend verkeer van persoonsgegevens is ingeregeld en persoonsgegevens buiten de beheersfeer van de verwerkingsverantwoordelijke en daarmee de organisatie raken.

Deze KPI kijkt op persoonsgegevensstromen van en naar betrokken partijen in verwerkingen. De onderbouwing van de rechtmatigheid van dit verwerken is een aspect waar de verwerkingsverantwoordelijke zich over dient uit te spreken en zijn maatregelenmix op moet inregelen. Documenteren hiervan vindt plaats in het register van verwerkingsactiviteiten conform en langs de vereisten van AVG art. 30.

Bij dit onderdeel is het van belang onderscheid te maken tussen:

- Een verwerkingsverantwoordelijke: stelt het doel (waarom?) en middelen (hoe?) vast van een verwerking.
- Een (sub)verwerker: een andere juridische entiteit die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke(n).

Uit het voorgaande kunnen dan drie soorten relaties worden onderscheiden:

- Verwerkingsverantwoordelijke – verwerker: de verwerkingsverantwoordelijk besteedt de verwerkingen uit aan een andere juridische entiteit. In dit geval moet een verwerkingsovereenkomst worden afgesloten.
- Twee verwerkingsverantwoordelijken: Een verwerkingsverantwoordelijke deelt gegevens met een partij die zelf doel en/of de middelen bepaald voor de verwerking. Een voorbeeld hiervan is het uitvoeren van een onderzoek. In dit geval moeten privacy afspraken worden afgesloten.
- Gezamenlijk verwerkingsverantwoordelijken: twee partijen stellen gezamenlijk het doel en de middelen voor de verwerking vast. In dit geval moeten privacy afspraken worden afgesloten.

Uit de PIA blijkt van welke relatie sprake is.

De KPI Betrokken partijen bestaat uit **vier** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

1 Afspraken maken en overeenkomsten sluiten met gebruik van modellen: de taken die een verwerkersverantwoordelijke en een verwerker in kader van de gegevensuitwisseling over en weer hebben worden in het kader van de AVG en de Wjsg vormgegeven door vastlegging van afspraken in (bilaterale of multilaterale) afsprakenkaders en verwerkersovereenkomsten.	
Onderbouwing kwaliteitsniveau:	Bij dit onderwerp wordt een onderscheid gemaakt tussen: • De contracten afgesloten door IVO • De contracten afgesloten door de individuele gerechten en diensten **IVO** De resterende verwerkersovereenkomsten worden in orde gemaakt. Er dienen nog voor enkele diensten verwerkersovereenkomsten te worden getekend. Daarbij dient te worden opgemerkt dat voor sommige diensten gezamenlijk een verwerkersovereenkomst moet worden opgesteld. Er zijn reminders verstuurd, de afdeling inkoop zit er bovenop. Helaas is het niet gelukt om alle overeenkomsten zoals gepland voor eind 2020 op te leveren. **Gerechten** Uit de beveiligingsbenchmark van gerechten 2019 van Motivaction d.d. 29 juli blijkt dat organisaties die te maken hebben met “verwerkers” bijna allemaal een verwerkersovereenkomst met externe partijen hebben. Dit is alleen niet het geval bij de Rechtbank Rotterdam, omdat daarvan geen statusupdate is ontvangen. Bij acht van de twintig organisaties is dit niet van toepassing. <u>Kwaliteitsniveau:</u> 4. Voor de meeste verwerkingen waarbij gegevens naar externe partijen worden verstuurd zijn verwerkersovereenkomsten of privacy-afspraken gemaakt

	voor zover nodig. Voor verwerkersovereenkomsten worden de ARBIT- of ARVODI-modellen van het Rijk gebruikt.
Ambitieniveau:	Ambitieniveau: 5. De Rechtspraak heeft nog niet voor alle externe datadelingen privacy-afspraken of een verwerkersovereenkomst opgesteld. Wel heeft de Rechtspraak in beeld waarvoor nog overeenkomsten afgesloten moeten worden. Hier wordt aan gewerkt. Acties: • De privacy officer van IVO blijft de ontwikkelingen inzake verwerkingsovereenkomsten en privacyafspraken nauwgezet volgen en ontvangt maandelijks een update van de contractmanager. • Bij de volgende KCD-uitvraag zal dit punt meegenomen worden (actie beleidsmedewerker privacy; 2e kwartaal 2021).
2 Documentatie onderlinge verhouding t.a.v. verwerking in keten- of andere samenwerking: is er sprake van gezamenlijke verwerkingsverantwoordelijkheid, wat voorkomt als twee of meerdere partijen doel en middelen van verwerken bepalen, moeten ook de onderlinge verhoudingen tot die verwerking worden gedocumenteerd in de registers van verwerkingsactiviteiten en de (bilaterale of multilaterale) afsprakenkaders.	
Onderbouwing kwaliteitsniveau:	Samenwerkingsverbanden zorgen ervoor dat persoonsgegevens buiten de organisatiemuren worden verwerkt. Zoals uit de introductie van dit hoofdstuk blijkt, kunnen deze samenwerkingsverbanden zich op verschillende manieren uiten. Gezamenlijke verantwoordelijkheid komt vooral voor in de relatie tussen de Raad voor de rechtspraak en de gerechten. In deze relatie is de onderlinge verhouding vastgelegd in diverse governance documenten. Zo ook voor5.1(2)h Verder zijn er weinig gevallen waarbij sprake is van gezamenlijke verwerkingsverantwoordelijkheid. Voor het opstellen van privacyafspraken en verwerkersovereenkomsten zijn procedures opgesteld door het LDCR en IVO. Het kwaliteitsniveau is gezien het bovenstaande 3.
Ambitieniveau:	Op dit moment zijn er geen signalen die nopen tot acties om het kwaliteitsniveau te verhogen.
3 Doorgifte persoonsgegevens aan een derde land: er moet duidelijkheid zijn welke waarborgen er zijn getroffen door de verwerkingsverantwoordelijke opdat het voor natuurlijke personen vereiste beschermingsniveau niet wordt ondermijnd.	
Onderbouwing kwaliteitsniveau:	Van doorgifte van persoonsgegevens aan een derde land is sprake wanneer persoonsgegevens buiten de Europese Economische Ruimte worden verwerkt. Denk hierbij aan het versturen of opslaan van persoonsgegevens in de Verenigde Staten. In dit kader zijn vier punten relevant. Ten eerste zijn er binnen de Rechtspraak 15 applicaties die persoonsgegevens buiten de Europese Economische Ruimte (EER) versturen. Door de vernietiging van het adequaatheidsbesluit (Privacy Shield) door het Hof van Justitie van de EU wordt op dit moment door IVO in kaart gebracht wat de impact daarvan is voor de Rechtspraak. Op basis van de resultaten worden verdere acties bepaald. Het aanpassen van bestaande verwerkersovereenkomsten als gevolg van de opheffing van het Privacy Shield is hier onderdeel van. Ten tweede is noemenswaardig de relatie met het Gemeenschappelijk Hof van Justitie van de Nederlandse Antillen. Op dit moment vinden nog geen gegevensuitwisselingen plaats tussen de Rechtspraak en het Gemeenschappelijk Hof. Er wordt wel in kaart gebracht welke

	mogelijkheden er zijn om het Gemeenschappelijk Hof gebruik te laten maken van verschillende faciliteiten die de Rechtspraak intern gebruikt. De privacyrisico's zijn hier duidelijk in beeld. Ten derde is het cloudbeleid voorgelegd aan de S&I Board. Het cloudbeleid van de Rechtspraak moet kaders bieden voor het gebruik van clouddiensten. Het stelt derhalve kaders aan de doorgifte van persoonsgegevens via informatiesystemen naar derde landen. Tot slot is als gevolg van de Brexit het Verenigd Koninkrijk een derde land. In het verdrag tussen de EU en het VK is een regeling opgenomen om ervoor te zorgen dat het uitwisselen van persoonsgegevens mogelijk blijft. Deze regeling is geldig voor 4 maanden en biedt een uitloopmogelijkheid tot 6 maanden. In deze periode moet een adequaatheidsbesluit worden opgesteld voor de AVG en Richtlijn 2016/680. De AP heeft voorafgaand aan de Brexit-deal een 'waarschuwing' afgegeven dat verwerkersovereenkomsten maatregelen moeten nemen als er geen adequaatheidsbesluit komt. De Rechtspraak moet, rekening houdend met scenario dat er niet tijdig een adequaatheidsbesluit is, alvast in kaart brengen welke gegevensverwerkingen plaatsvinden naar het VK. Kwaliteitsniveau: 4.
Ambitieniveau:	Er worden nadere verwerkersovereenkomsten opgesteld voor de bestaande diensten in de Amerikaanse cloud. Nieuwe diensten die de cloud in willen moeten daarvoor eerst langs de cloudregiegroep om daarvoor goedkeuring te krijgen. Voor de nieuwe Amerikaanse clouddiensten geldt dat in de verwerkersovereenkomst rekening moet worden gehouden met de opheffing van het privacy shield. Hiervoor is de standaard verwerkersovereenkomst aangepast. Zowel bij bestaande Amerikaanse clouddiensten als nieuwe Amerikaanse clouddiensten zal voorts moeten worden bezien of (technische) maatregelen genomen moeten worden of zijn zoals encryptie. Er wordt rekening mee gehouden in het cloudbeleid. Het cloudbeleid wordt op 2 februari besproken in de S&I board. Ambitieniveau: 5.
4 **Borgen informatiepositie en uitoefening rechten betrokkenen:** voor betrokkenen dient het bestaan van meerdere partijen geen onderscheid op te leveren om zijn rechten als betrokkene te kunnen uitoefenen (het bij elke partij aan kunnen kloppen met vragen over de verwerking) maar ook hoe en door wie invulling wordt gegeven aan de informatieplicht van partijen.	
Onderbouwing kwaliteitsniveau:	Ook wanneer sprake is van een samenwerkingsrelatie (zie 2) moeten de rechten van betrokkenen worden gewaarborgd. Hierover moet het een en ander in de verwerkersovereenkomsten of privayafspraken worden vastgelegd Artikel 8 van de ARBIT- en ARVODI- template welke door de Rechtspraak wordt gebruikt, bepaalt dat de wederpartij zal ondersteunen bij de uitvoering van de rechten van betrokkenen. In dezelfde template wordt steeds opgenomen wie de wederzijdse contactpersonen zijn. Hiermee wordt de mogelijkheid van betrokkenen om de wettelijke rechten uit te oefenen gewaarborgd. Betrokkenen worden niet proactief geïnformeerd over de partijen waarmee de Rechtspraak overeenkomsten heeft afgesloten.

	Kwaliteitsniveau: 3
Ambitieniveau:	Op dit moment heeft de Rechtspraak nog geen signalen om het kwaliteitsniveau te verhogen.

8. Overige onderwerpen

Bij de J&V-indicatoren werden nog enkele andere punten benoemd die relevant zijn om te blijven monitoren, maar geen plek hebben gekregen in de privacy management KPI's. In dit hoofdstuk worden die onderwerpen voor de volledigheid behandeld.

a. Coronacrisis

Naar aanleiding van de verspreiding van COVID-19 heeft het kabinet in maart 2020 verschillende maatregelen afgekondigd. Het gevolg van deze maatregelen is onder andere dat rechtbanken alleen nog open zijn voor urgente zaken en dat het verzuim om verschillende redenen is toegenomen.

COVID-19 noodzaakt de gerechten maatregelen te nemen om ervoor te zorgen dat de bedrijfsvoering zo veel mogelijk doorgaat. De privacywetgeving blijft ook in tijden van crisis gelden en het is van belang dat de gerechten bij het nemen van de maatregelen hieraan, ondanks de crisis, blijven voldoen.

Met de versoepeling van de maatregelen is het ook weer mogelijk voor de gerechten om langzaam meer zittingen te laten plaatsvinden. Hiervoor is het een en ander voorbereid door het CMT, SBO en het LOBRO. Zo krijgt ieder gerecht een eigen register. In dit register wordt zes weken lang bewaard wie als publiek aanwezig is geweest bij een zitting. Bij een eventuele besmetting van een aanwezig persoon kan de Rechtspraak bijdragen aan het contactonderzoek. Op dit proces is een PIA Light uitgevoerd die is voorgelegd aan het PRO.

Acties (beleidsmedewerker privacy/FG; doorlopend gedurende de coronacrisis):

1. welke verwerkingen naar aanleiding van COVID-19 extra plaatsvinden;
2. toetsen of de verwerkingen rechtmatig gebeuren;
3. de gerechten adviseren wanneer gegevens in meer of mindere mate onrechtmatig worden verwerkt.

b. Vragen AP sectorbeeld politie en justitie

Door de Autoriteit Persoonsgegevens zijn vragen gesteld aan de Rechtspraak om een beeld te krijgen van de stand van dataprotectie binnen de sector Politie en Justitie. De beantwoording van deze vragen is door het Bureau Raad, samen met het privacyteam van IVO, voorbereid.

Op 9 november is de reactie vanuit het Bureau Raad verstuurd aan de AP. Daarnaast is de reactie ook gedeeld met de PGHR en de controller van het ministerie van Justitie en Veiligheid. Er is nog geen reactie ontvangen.

Deelbesluit 1 - Datalekken
Document 9

(7E) Borgingsplan Privacy Rechtspraak

Versie 1 juli 2021

Inhoud

1. Afkortingen

AVG	Algemene verordening gegevensbescherming (EU- verordening 2016/679).
ARBIT	Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten.
ARVODI	Algemene Rijksinkoopvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten.
BVA	Beveiligingsautoriteit.
BVC	Beveiligingscoördinator.
BSD	Basis Selectie Document.
CISO	Chief information security officer.
CIO	Chief information officer.
FG	Functionaris gegevensbescherming.
HR(M)	Human Resource (Management).
IVO Rechtspraak	Informatievoorzieningsorganisaties Rechtspraak.
JenV	Ministerie van Justitie en Veiligheid.
KCD	Key Control Dashboard.
KPI	Kritieke prestatie-indicatoren.
LBVr	Landelijk Bureau Vakinhoud rechtspraak.
LDCR	Landelijk Dienstencentrum Rechtspraak.
(DB) LOBRO	(Dagelijkst bestuur) Landelijk Overleg Beveiligingscoördinatoren Rechterlijke Organisatie.
PbD	Privacy by Design.
PDCA-cyclus	Plan-Do-Check-Act-cyclus.
PGHR	Procureur-Generaal bij de Hoge Raad.
PIA	Privacy Impact Assessment.
PRO	Presidenten-Raad Overleg.
Rvdr	Raad voor de rechtspraak.
SBO	Strategisch Bedrijfsvoeringsoverleg.
SP&K	Security, privacy & Kwaliteit.
S&I-Board	Strategie en Innovatie board.
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming.
Wjsg	Wet justitiële en strafvorderlijke gegevens.

1. Inleiding

Aanleiding

Het uitgangspunt van de Rechtspraak ten aanzien van privacy is om altijd in lijn met de geldende wet- en regelgeving te handelen. Dit kader wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), Wet justitiële en strafvorderlijke gegevens (Wjsg) en het bijbehorende besluit.

Voorafgaand aan de inwerkingtreding van de AVG is het Bureau Raad het Project AVG gestart om de overgang naar de AVG te structureren en te borgen. Na de inwerkingtreding van de AVG is het project gestopt. De werkzaamheden worden in de lijn verder opgepakt.

Doel

Om inzicht te behouden in de nog openstaande punten, is het borgingsplan privacy opgesteld. Hierin staat welke activiteiten nog moeten worden ondernomen om in lijn met de privacywetgeving te handelen en het handelen als zodanig te borgen.

Herijking

Om het doel van het borgingsplan te volbrengen, wordt het plan minimaal halfjaarlijks herijkt. Hierdoor blijft het borgingsplan een actueel beeld geven van de werkzaamheden die ten aanzien van privacy nog moeten worden verricht. Daarbij wordt ook zo goed als mogelijk inzage gegeven in de planning per actie.

Nadat het eerste borgingsplan in januari 2019 is vastgesteld, is het onderhavige document de zevende versie.

KPI’s

De kritieke prestatie-indicatoren (KPI’s) staan beschreven in JenV-document ‘Privacymanagement-KPI's’, pilotversie 0.9 (juli 2020). De KPI’s en handreiking zijn onderdeel van het instrumentarium voor privacymanagement van JenV. Om te toetsen of dit instrumentarium werkbaar is in de uitvoering loopt JenV-breed een pilotjaar van juli 2020-juli 2021. Met inachtneming van de bijzondere positie van de Rechtspraak hanteren we deze KPI’s vanwege de vergelijkbaarheid en omdat het een handig instrument vormt om voortgang inzichtelijk te maken.

In april 2021 is een nieuwe versie van de KPI’s aangeboden aan de CIO-Raad JenV van 20 mei 2021. Deze versie wordt hier nog niet gebruikt. Pas bij definitieve vaststelling van de KPI’s wordt daar wederom op aangesloten.

Leeswijzer

Het vervolg van het document is als volgt. In hoofdstuk 2 wordt een algemeen beeld gegeven over de implementatie en borging van de privacywet- en regelgeving binnen de Rechtspraak. In hoofdstuk 3 wordt ingegaan op hoe en door wie het borgingsplan wordt samengesteld. Vervolgens wordt in hoofdstuk 4 tot en met 7 op basis van de vier privacy management KPI’s van JenV de status ten aanzien van privacy weergegeven. Tot slot worden in hoofdstuk 8 nog enkele onderwerpen behandeld die relevant zijn voor de Rechtspraak, maar niet passen in een van de KPI’s.

2. Beeld Rechtspraak

Er is al veel werk verzet, maar er is ook nog genoeg te doen. Om het algemeen beeld van de Rechtspraak uit te drukken wordt gebruik gemaakt van de termen: ‘in-control’ en ‘compliant’. Met dit eerste wordt bedoeld dat nog niet op alle onderdelen aan de geldende privacywet- en regelgeving wordt voldaan, maar dat wel duidelijk is wanneer hieraan voldaan wordt. Met dit tweede wordt bedoeld dat alle aan onderdelen van de privacywet- en regelgeving wordt voldaan en dat de onderdelen zijn geborgd. Hierbij moet de kanttekening gemaakt worden dat nooit sprake kan zijn van 100% compliancy. De stand van de techniek en de interne en externe omgeving veranderen dusdanig snel dat altijd ruimte is voor verbetering. Borgen staat daarom centraal.

Het Bureau BVA concludeert dat de Rechtspraak niet in-control of compliant is met de geldende privacywet- en regelgeving. Dit komt door een gebrek aan inzicht in het IT-landschap en een heldere planning om de informatievoorziening in lijn met de geldende privacywet- en regelgeving te brengen. Om in-control te zijn zal de Rechtspraak ervoor moeten zorgen dat er zicht is op de volledige informatievoorziening. Tegelijkertijd moet er een eenduidige planning zijn om de systemen in de informatievoorziening in lijn te brengen met de privacywet- en regelgeving. Bij dit laatste bestaat de mogelijkheid om systemen, na een risicoafweging, niet meer aan te passen, omdat ze op korte termijn zullen worden uitgefaseerd.

Om compliant te worden, zal de Rechtspraak de actiepunten in dit plan moeten borgen.

3. Werkwijze en totstandkoming

Dit plan is ingedeeld conform de privacy management KPI's vanuit het ministerie van Justitie en Veiligheid (JenV). KPI worden verschillende aandachtspunten behandeld. Deze scoring vindt plaats op twee niveaus: het kwaliteitsniveau en het ambitieniveau. De scoringsniveau's gaan van 1 (laagst) t/m 5 (hoogst)..

Kwaliteitsniveau
Ieder aandachtspunt krijgt een score voor het kwaliteitsniveau dat past bij de huidige situatie. De score wordt onderbouwd aan de hand van voorbeelden (zoals bestaande afspraken, procedures, processen, diensten en producten). Hieruit moet de passendheid van het aangegeven kwaliteitsniveau blijken.

Ambitieniveau
In relatie tot het kwaliteitsniveau wordt aangegeven wat bij ieder aandachtspunt de ambitie van de Rechtspraak is. Hierbij wordt aangegeven welke acties nodig zijn om tot dat niveau te komen. Aan iedere actie wordt een actiehouder en een deadline gekoppeld, zodat periodiek de voortgang wordt vastgesteld. Tegelijkertijd zorgt een actie ervoor dat privacy wederom aandacht en prioriteit krijgt.

Overall-aanpak
Dit borgingsplan is opgesteld in opdracht van de Raad voor de rechtspraak. Opdrachtnemer is de directeur van het Bureau van de Raad voor de rechtspraak.

De uitvoering van de activiteiten wordt gecoördineerd door een werkgroep met daarin de volgende deelnemers:

- Functionaris gegevensbescherming
- Privacy officer IVO
- Functionarissen privacy IVO
- Teamleider security, privacy & kwaliteit IVO/ Chief Information Security Officer (CISO)
- Beleidsmedewerker privacy bureau Rvdr
- Lead adviseur IV-strategie en -beleid (CIO office)
- (senior)adviseurs Recht & ICT afdeling Strategie Bureau Rvdr

Agendalid: stafmedewerker Europees recht Landelijk Bureau Vakinhoud rechtspraak

De daadwerkelijke uitvoering van de activiteiten ligt bij een veel grotere groep medewerkers waarbij medewerkers op het terrein van informatiebeveiliging, service delivery, architectuur, applicatiebeheer, inkoop, portefeuillehouders en de lokale privacycoördinatoren bij de gerechten belangrijke partijen zijn.

Beperkingen
Het plan gaat niet in op de werkzaamheden van het Landelijk Bureau Vakinhoud rechtspraak (LBVr), waarbij het gaat om de werkzaamheden die liggen in het verlengde van het werk van de rechter. Hiervoor is de werkgroep AVG vakinhoud opgericht die bestaat uit experts vanuit de gerechten. Vanzelfsprekend is er wel samenwerking met en uitwisseling van kennis tussen het LBVr en de betrokkenen vanuit (de bedrijfsvoering van) de Rechtspraak.

Disclaimer
De pilot van JenV die in het bovenstaande kader werd genoemd, wordt door de Rechtspraak gebruikt om te bepalen of deze werkwijze voor de Rechtspraak werkbaar is. Er is dan ook nog geen bestuurlijke goedkeuring gegeven op de genoemde scores. De pilotfase zal worden afgerond op 1 juli 2021. Daarna worden de resultaten besproken in het CIO-beraad (van de CIO Rijk). Na vaststelling door het CIO-beraad kan de Rechtspraak besluiten over de werkbaarheid en de scoring van de kwaliteits- en ambitieniveaus.

4. Privacyadministratie

De KPI privacyadministratie omvat alle aandachtsgebieden voor de Rechtspraak die een rol spelen bij het kunnen aantonen van en verantwoorden over de naleving c.q. het compliant werken aan van privacy wet- en regelgeving (Verantwoordingsplicht). Aan de hand van de aandachtsgebieden bij deze KPI geeft de verwerkingsverantwoordelijke inzicht in de status quo van de wettelijk verplichte documentatieopbouw voor deze aandachtsgebieden (Documentatieplicht) en laat naar buiten zien wat er zoal op de rit is als onderbouwing voor de door de organisatie gehanteerde zorgvuldigheid in haar omgangsvormen met persoonsgegevens.

De KPI bestaat uit **zes** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

1 **Register van verwerkingsactiviteiten:** Hierin ligt de onderbouwing van de rechtmatigheid van verwerkingen vast.	
Onderbouwing kwaliteitsniveau: 3	De privacywet- en regelgeving stelt als eis dat persoonsgegevens rechtmatig worden verwerkt en dat dit aantoonbaar is. Het register van verwerkingsactiviteiten geeft in een overzicht een integraal beeld van alle verwerkingen door een (of meerdere) verwerkingsverantwoordelijken. Per verwerking wordt aangegeven wat het doel is, welke (wettelijke) grondslag van toepassing is, hoe lang de persoonsgegevens worden bewaard, etc. Voorafgaand aan de inwerkingtreding van de AVG is door de projectleiding van het AVG-project van het Bureau Rvdr een landelijk verwerkingenregister opgesteld. Het landelijk register bevat de gemeenschappelijke gegevensverwerking door de Rechtspraak. Daarnaast heeft ieder gerecht onder eigen verantwoordelijkheid een lokaal register waarin de verwerkingen staan die naast de Rechtspraakbrede verwerkingen plaatsvinden. In dat kader is in samenwerking met IVO, gerechten en diensten het volgende gerealiseerd: ✓ Landelijk register: IT-applicaties (beheer IVO); ✓ Lokale registers: lokale IT en registraties (beheer gerechten en landelijke diensten zelf). Een samenvatting is te vinden via: register van verwerkingen Deze registers waren 25 mei 2018 (nagenoeg) afgerond. De Rvdr is als verwerkingsverantwoordelijke verantwoordelijk voor het vullen van het landelijke register. Het bijhouden en verder vullen omtrent de verwerkingen die landelijk plaatsvinden is door de Rvdr gemandateerd aan de privacy officer van IVO. **Landelijk register** Het landelijk register van verwerkingen is nagenoeg ingevuld en wordt op basis van nieuwe inzichten en nieuwe initiatieven constant bijgewerkt. **Lokale registers** Er is in mei 2020 een inventarisatie geweest van de lokale registers door de beleidsmedewerker privacy van het bureau Rvdr om te onderzoeken in hoeverre de lokale registers voldoen aan de geldende privacywetgeving. In mei 2021 heeft een nieuwe inventarisatie plaatsgevonden. In beide gevallen is hiervoor het Key Control Dashboard gebruikt. Op basis van de inventarisatie van 2020 werd de conclusie getrokken dat de meeste gerechten en diensten een eerste stap gezet met het register van verwerkingsactiviteiten. De registers gingen per verwerking echter niet in op alle vereisten uit de AVG. De gerechten en diensten zijn via de BVC'ers hierop

	geattendeerd. Uit de inventarisatie van 2021 blijkt dat drie gerechten aantoonbaar stappen hebben gemaakt. Andere gerechten werken nog aan een nieuwe inventarisatie of hebben het register niet aangeleverd of bijgewerkt. Wederom zullen deze gerechten hierop worden geattendeerd. In 2022 wordt een nieuwe inventarisatie uitgevoerd. De BVC'ers zullen hierover worden geïnformeerd. Indien er dan geen aantoonbare vooruitgang geboekt is, zal dit worden teruggekoppeld aan het niet-rechterlijk bestuurslid.
Ambitieniveau: 5	**Borging en vervolgstap** De Rechtspraak moet ervoor zorgen dat alle lokale en landelijke verwerkingen zijn geïnventariseerd en worden bijgehouden. Bij de meeste gerechten is dit inzicht op lokaal niveau aanwezig. Ook op landelijk niveau is het register nagenoeg ingevuld. Hierna kan de vervolgstap gemaakt worden dat overbodige verwerkingen worden beëindigd, dat het register constant wordt bijgehouden en dat er een PIA is voor iedere verwerking in het register. De tool SmartPIA zal hierbij helpen. **Beperking** Volgens de privacy governance is ieder gerecht en iedere dienst zelf verwerkingsverantwoordelijk. Deze verwerkingsverantwoordelijkheid is verder uitgewerkt in andere documenten, zoals het bijbehorende Addendum. Een centraal register van verwerkingen met daarin alle verwerkingen van alle gerechten past niet binnen dit uitgangspunt. Hiervoor moet de volgende acties worden uitgevoerd: • Implementatie van SmartPIA (Samenwerking Bureau Raad en IVO, Q4 2021 & Q1 2022) • In het tweede kwartaal van 2022 wordt bij de gerechten opnieuw nagegaan of de lokale registers van verwerkingsactiviteiten zijn verbeterd voor zover nodig
2 **DPIA's:** hiermee wordt gemonitord dat de risico-inschattingen van verwerkingen aanwezigheid is en kwalitatief adequaat zijn. Dit geeft de verwerkingsverantwoordelijke inzicht in de risico's en zorgt ervoor dat de risico's worden teruggebracht naar een voor de verwerkingsverantwoordelijke acceptabel niveau.	
Kwaliteitsniveau: 2	De status van dit aandachtspunt wordt uitgesplitst naar de situatie bij: 1) IVO Rechtspraak; 2) het LDCR; en 3) de gerechten en overige diensten. 4) alle Rechtspraakonderdelen Hierbij kan opgemerkt worden dat PIA's plaatsvinden conform het Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA). Daarnaast wordt in sommige gevallen gebruik gemaakt van de PIA Light. **1. IVO Rechtspraak** De Rechtspraak maakt gebruik van een mix van oudere en nieuwe systemen. Deze systemen worden veelal door IVO Rechtspraak beheerd. Van de oude systemen zijn voor de invoering van de AVG en de Wjsg geen PIA uitgevoerd. De PIA's die wel zijn uitgevoerd, zijn veelal niet meer actueel. Deze PIA's worden met terugwerkende kracht alsnog opgesteld en bijgewerkt. Voor nagenoeg alle primaire processystemen is in 2019 en 2020 een PIA opgesteld. Daarnaast zijn er ook PIA's uitgevoerd op de secundaire processystemen. Het is echter onduidelijk of op alle systemen reeds een PIA is uitgevoerd. Om nieuwe omissies te voorkomen wordt sinds 2016 elk nieuw (te ontwikkelen) systeem onderworpen aan een PIA. Bij aanpassingen wordt de bestaande PIA herijkt.

Om het proces voor het uitvoeren van PIA's te borgen is door IVO een procesbeschrijving opgesteld. De procesbeschrijving gaat in op het uitvoeren van PIA's voor nieuwe projecten, bestaande diensten en de periodieke herijking van PIA's. Dit is een samenwerking waar ook vertegenwoordigers vanuit de business bij aansluiten. Verder wordt de tool SmartPIA geïmplementeerd en geïntroduceerd. Deze tool maakt het uitvoeren van PIA's eenvoudiger en het structureert de management van privacy.

2. LDCR

Het LDCR verzorgt onder andere de inkoop van producten en diensten voor gerechten. Voor het overgrote deel van de verwerkingen die worden ingekocht, worden in meer of mindere mate persoonsgegevens verwerkt. Deze verwerkingen moeten conform de privacywet- en regelgeving plaatsvinden. Dit betekent dat met terugwerkende kracht moet worden gecontroleerd dat voor iedere afgenomen dienst een PIA is uitgevoerd en een verwerkersovereenkomst (indien nodig) is afgesloten.

Sinds de inwerkingtreding van de privacywet- en regelgeving is door het LDCR een werkproces opgesteld voor verplichtingen uit deze wet- en regelgeving in het de aankoop- en aanbestedingstrajecten. Verder heeft de inkoopafdeling van het LDCR een inhaalslag gemaakt om qua PIA's en verwerkersovereenkomsten aan de AVG-verplichtingen te voldoen. Er is nog een overeenkomst waarbij voldaan moet worden aan de AVG-verplichten.

Voor alle andere landelijke contracten is bepaald of er een PIA moet plaatsvinden en/of een verwerkersovereenkomst moet worden opgesteld. Bij nieuwe overeenkomsten wordt gecontroleerd of een PIA gedaan is en of een verwerkersovereenkomst moet worden opgesteld.

3. Gerechten en overige diensten

Ieder gerecht heeft een register van lokale verwerkingsactiviteiten (zie hiervoor). Aan iedere verwerking in het register moet een PIA ten grondslag liggen waaruit de informatie voor het register blijkt. Denk aan het doel van de verwerking, de bewaartermijn en de ondersteunende systemen.

Ter controle van dit proces is in april 2020 via het Key Control Dashboard (KCD) uitgevraagd in hoeverre de nodige lokale PIA's zijn uitgevoerd. Uit de uitvraag is gebleken dat PIA's nog onvoldoende plaatsvinden vanwege een gebrek aan kennis. Daarom is eind september 2020 een cursus gegeven aan de privacycoördinatoren om de benodigde kennis bij te brengen. Begin 2021 heeft een vervolgcursus plaatsvonden. Hierin is ook het cyclische karakter van de PIA besproken. Inmiddels hebben verschillende gerechten ervoor gekozen om gezamenlijk capaciteit beschikbaar te maken voor het bijwerken van het register van verwerkingsactiviteiten en het opstellen van PIA's.

Ondanks dat bij de gerechten PIA's nog onvoldoende plaatsvinden, wordt het overgrote deel van de verwerkingen afdekt met PIA's die door IVO uitgevoerd. Daarnaast signaleert het LDCR als een PIA ontbreekt bij de aankoop van een nieuwe dienst of systeem. Het LDCR geeft dit bij het betreffende gerecht aan.

4. Alle Rechtspraakonderdelen

Als de PIA is uitgevoerd, moet de PIA bestuurlijk worden vastgelegd. Uit de Privacy Governance Rechtspraak blijkt dat in geval van een gerechtsoverstijgende PIA de Raad en de gerechtsbesturen als gezamenlijk

	verwerkingsverantwoordelijken de PIA moeten goedkeuren. Het voorleggen van een PIA aan (veelal) het PRO is echter niet voor iedere PIA noodzakelijk is. Aan vereenvoudigingsstructuur wordt gewerkt.
Ambitieniveau: 3	Er zijn twee verbeteracties te onderscheiden: 1) <u>Bestuurlijke vaststelling van PIA's en de acceptatie/mitigatie van risico's</u> Het reeds vastgestelde Addendum Privacy Governance wordt op basis van het voorstel vanuit het BVA aangevuld met een mandateringsstructuur om het vaststellen van PIA's en de bijbehorende risico's te vereenvoudigen. Deze aanvulling zal tegelijkertijd met de PIA E-archief aan het PRO worden voorgelegd. 2) <u>Implementatie PIA-tool:</u> In 2021 wil de Rechtspraak gebruik gaan maken van een PIA tool. Deze tool zal: - het PIA-proces versnellen door het automatiseren; - de kwaliteit verbeteren doordat de tool de gebruiker kennis aanreikt; - signaleren als een PIA na een bepaalde periode moet worden herijkt; - automatisch het register van verwerkingsactiviteiten bijwerken. De tool is aangekocht en er is capaciteit beschikbaar gemaakt om de tool te implementeren. Op 26 mei is het implementatietraject met een kick-off begonnen. Hiervoor moeten de volgende acties worden uitgevoerd: • Afronden implementatie PIA-tool (IVO/bureau Raad, Q4 2021 en Q1 2022) • Mandateringsstructuur PIA (beleidsmedewerker privacy, september 2021).
3 **Toestemmingsregister:** binnen dit aandachtspunt gaat het over de aanwezigheid en kwaliteit van registraties waaruit de omgang met toestemming voor het verwerken van persoonsgegevens (en het weer kunnen intrekken daarvan) blijkt.	
Onderbouwing kwaliteitsniveau: 2	**De rol van toestemming voor de Rechtspraak** Toestemming in de zin van de AVG heeft voor de Rechtspraak, vergeleken met andere organisaties, een beperkte rol. De verwerkingen van de Rechtspraak worden namelijk grotendeels gebaseerd op de grondslagen: - wettelijke verplichting (art. 6, lid 1, sub c AVG); en - de taak van algemeen belang (art. 6, lid 1 sub e AVG). Bij innovatieve projecten of in de bedrijfsvoering heeft toestemming als grondslag een iets grotere rol. **Documentatie van toestemming** Dit onderdeel is tweeledig. Enerzijds moet toestemming als grondslag in het register van verwerkingsactiviteiten bij een verwerking worden opgenomen. Over het register van verwerkingsactiviteiten is hiervoor al het een en ander gezegd (zie aandachtspunt 1). Anderzijds is het van belang dat de Rechtspraak de grondslag toestemming adequaat toepast. Ieder gerecht en elke dienst is hiervoor zelf verantwoordelijk. In de KCD-uitvraag is aan de gerechten en diensten gevraagd of zij duidelijk in beeld

	hebben in welke gevallen toestemming als grondslag wordt gebruikt. De meeste gerechten en diensten hebben dit overzicht. Toestemming wordt slechts in een aantal verwerkingen gebruikt. Meest voorkomend het faciliteren van opleidingen, bepaalde lijsten en HR-processen.
Ambitieniveau: 3	Voor de Rechtspraak is het van belang dat voor ieder gerecht en voor iedere landelijke dienst te allen tijde duidelijk is bij welke verwerkingen de grondslag toestemming wordt gebruikt en dat het proces hieromtrent vastgelegd en geborgd is. De gerechten en diensten moeten ervoor zorgen dat dit in de registers van verwerkingsactiviteiten is geborgd en de toepassing kunnen aantonen. Actie: • Bij de terugkoppeling op de KCD-uitvraag ontvangen de gerechten bij wijze van herinnering de kaders voor het gebruik van de grondslag toestemming. (Beleidsmedewerker privacy & informatiebeveiliging, 2e kwartaal 2021).
4 **Datalekregister:** de wijze waarop informatiebeveiligingsincidenten worden gedocumenteerd, beheerd en qua afhandeling (waaronder de kwalificatie datalek toekenning) worden bewaakt	
Onderbouwing kwaliteitsniveau: 4	Sinds de zomer van 2016 is er een procedure voor het melden van datalekken. In oktober 2019 is deze procedure vernieuwd in het handboek datalekken. De beveiligings- en privacycoördinatoren bij gerechten en diensten zijn verantwoordelijk voor de uitvoering van de procedure. Het registeren gebeurt op dit moment nog met behulp van het softwarepakket Classbase. Op het initiatief van het LOBRO is er door IVO een sharepointsysteem ontwikkeld waarmee de registratie van datalekmeldingen geüniformeerd is. Dit systeem heeft als voordeel dat eventuele meldingen naar de toezichthouder direct gegenereerd kunnen worden. Met de Hoge Raad zijn afspraken gemaakt dat het formulier uit dit systeem door hen wordt geaccepteerd. De FG en de BVA zorgen, met hulp van de Medewerker BVA, voor overzichten ten behoeve van de viermaandsrapportage en het jaarverslag. Deze rapportages worden gedeeld met het LOBRO en het SBO, zodat zij kunnen kennisnemen van de resultaten en de daarop gebaseerde adviezen. Veel van de datalekken hangen samen met het onvoldoende anonimiseren van uitspraken die gepubliceerd worden of met het verkeerd versturen van documenten. Om het aantal datalekken te verminderen en vanwege de ambitie van de Raad van State, de Hoge Raad en de Rechtspraak om meer uitspraken te publiceren werkt IVO aan een anonimiseertool. Een tool is hiervoor reeds aangekocht. In het kader van het implementatietraject wordt binnenkort gestart met een experiment om de werking van de tool te controleren. Op 5 juli 2021 is hierover door de plv. FG positief geadviseerd.
Ambitieniveau: 5	Het landelijk overleg van BVC'ers, het LOBRO, heeft een inventarisatie gedaan waaruit blijkt hoe er bij de gerechten omgegaan wordt met verwerking, registratie en meldingen van datalekken. Uit de cijfers over meldingen blijkt een verschil in aanpak per gerecht. Om te komen tot een uniforme werking is het sharepointsysteem ontwikkeld. Er is echter nog een verschil in de gevallen waarin melding wordt gedaan bij de toezichthouder. Het ene gerecht meldt alles en sommige gerechten uitsluitend 'ernstige' datalekken. Dit zal door het (DB) LOBRO met de PGHR worden besproken.

	Acties: • Afspraken uniforme melding datalekken (LOBRO; eind 4e kwartaal 2021) • Experiment en landelijke uitrol anonimiseertool (projectleider bij IVO; uitrol begint – onder voorwaarde – in 2022).
5 Gegevensbeschermingsbeleid Hiermee wordt het voor iedereen binnen de organisatie duidelijk hoe met persoonsgegevens wordt omgegaan.	
Onderbouwing kwaliteitsniveau: 3	Het privacybeleid wordt in meerdere documenten op meerdere niveaus vormgegeven: - Strategisch niveau: o Strategisch plan privacy[1] o Beveiligingsbeleid voor de Rechtspraak 2019-2023 - Tactisch niveau: o Minimumnormen beveiliging en privacy o IT-normenkader o Evt. intern beleid (bijv. Privacybeleid IVO) - Operationeel niveau: o Procesbeschrijvingen en best practices Het beleid wordt periodiek herijkt. Hieronder wordt nader ingegaan op de implementatie van de BIO en de verwerking van persoonsgegevens door HRM, inkoop en externe onderzoeken. **BIO** Nadat IVO Rechtspraak in januari 2020 is overgestapt op de BIO, hebben de gerechten en andere diensten ook besloten over te stappen naar de BIO. Om de gerechten en diensten bij de overgang naar de BIO te ondersteunen, wordt door het Bureau BVA in kaart gebracht welke minimumnormen moeten worden aangepast aan de BIO te voldoen. Deze inventarisatie is afgestemd met IVO en is op 27 mei in het LOBRO besproken. Vaststelling van de gewijzigde minimumnormen door het SBO wordt nu voorbereid. Verder wordt door IVO geïnventariseerd wat zij aan IT-securitybeleid moeten aanpassen om het beleid in lijn te brengen met de BIO. Momenteel wordt een nulmeting uitgevoerd op de dienst om te zien waar de hiaten zitten. Verder wordt de PDCA-cyclus ingericht om in control te komen en te blijven. De BIO wordt per hoofdstuk vertaald naar handreikingen (intern beleid). Logging is daarbij als eerste opgepakt. **Verwerking van personeelsgegevens** Door de HRM-afdelingen, Inkoop en externe onderzoekers binnen de Rechtspraak worden veel (vertrouwelijke) persoonsgegevens verwerkt. Het is van belang dat deze gegevens rechtmatig worden verzameld, rechtmatig worden verwerkt en tijdig worden verwijderd. Naar aanleiding van signalen dat persoonsgegevens onveilig worden verstuurd, is het van belang om hier extra aandacht aan te besteden. Door de beleidsadviseur privacy en de FG is hierover gesproken met de manager HRM&OO. Afgesproken is om de HR-processen in drie fases aan te pakken: 1) Functioneringsgesprekken rechterlijke ambtenaren

[1] Vastgesteld door het PRO in september 2017.

	2) Andere HR-processen rechterlijke ambtenaren 3) Andere gerechtelijk ambtenaren
Ambitieniveau: 5	Verbeteringen zijn gelegen in: - het meer actief uitdragen van het privacybeleid door de besturen en directies en het faciliteren van opleidingen; en - verbeteren van de procedures en gegevensverwerking in het kader van HRM, inkoop en onderzoeken. Acties: - Faciliteren van de overstap naar de BIO voor de gerechten (beleidsmedewerker privacy & informatiebeveiliging; 4e kwartaal 2021). - Borgen privacy in HR-processen en bij externe onderzoeksaanvragen. (FG/Adviseur privacy & informatiebeveiliging; 2e kwartaal 2022)
6 Privacyverklaring Met een privacyverklaring wordt de informatieplicht over het verwerken van informatie door de verwerkingsverantwoordelijke naar betrokkenen vormgegeven.	
Onderbouwing kwaliteitsniveau: 2	Door de Rechtspraak is de algemene privacyverklaring gepubliceerd op rechtspraak.nl. De informatie hierin is uitgesplitst per rechtsgebied. Daarnaast is onlangs op de vacaturepagina van de Rechtspraak een aparte privacyverklaring gepubliceerd.
Ambitieniveau:3	Om het ambitieniveau te halen, moet de Rechtspraak meer grip krijgen op gegevensverwerkingen die naast het primaire proces plaatsvinden, zoals het wervings- en selectietraject. Hierna kan de informatieplicht hierop worden aangepast. De realisatiedatum van deze ambitie is afhankelijk van de samenwerking met o.a. teams HRM, Inkoop en externe onderzoeken. Verder is dit ambitieniveau ook afhankelijk van het werk bij de gerechten. Uiteindelijk zal volgens een cyclisch proces de privacyverklaring worden bijgewerkt. Gezien de datum van de actie in het vorige ambitieniveau, kan een eerste aanpassing verwacht worden in het 2e of 3e kwartaal 2021. Een definitieve einddatum kan niet worden gegeven.

5. Transparantie

De KPI Transparantie geeft aan op welke wijze de verwerkingsverantwoordelijke namens diens organisatie invulling geeft aan het transparantiebeginstel, dat onderdeel uitmaakt van de Rechten van Betrokkenen. Transparantie is een onderdeel van de informatieplicht die op de verwerkingsverantwoordelijke rust en gaat over gepaste openheid over de gehanteerde zorgvuldigheid bij het verwerken van persoonsgegevens.

De wijze van informatieverstrekking wordt situationeel bepaald en is een belangenafweging. Dit kan persoonlijk en al dan niet 'just-in-time' (mondeling, brief, aanreiken van flyer, digitaal/internet) of indirect en meer algemeen via een privacyverklaring worden vormgegeven, waarbij vereiste informatie voor betrokkenen op of vanuit één plek vindbaar is dan wel wordt aangeboden. Dit informeren gaat in principe altijd vóóraf aan het verwerken van persoonsgegevens van betrokkenen door of namens de verwerkingsverantwoordelijke. Dat dit heeft plaatsgevonden is aantoonbaar.

De KPI Transparantie bestaat uit **drie** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

1 **Inhoud informatie:** dit omvat **wat** wordt vastgelegd (instroom) en **waarom**, **wie** er toegang heeft tot deze informatie en/of aan wie en waarom worden welke persoonsgegevens verstrekt (doorstroom) maar ook het aangeven hoe lang persoonsgegevens worden bewaard en **wanneer** en op **welke** wijze deze persoonsgegevens weer worden verwijderd, vernietigd en/of gearchiveerd (uitstroom).	
Onderbouwing kwaliteitsniveau: 3	Bij dit aandachtspunt gaat het over de informatie die onder andere in de privacyverklaring is opgenomen. Op rechtspraak.nl/privacy worden de 5w- en h- vragen beantwoord onder de veel gestelde vragen. Verder gelden voor de bewaartermijnen van documenten in het primaire proces de basisselectiedocumenten. Deze zijn gepubliceerd op nationaalarchief.nl
Ambitieniveau: 4	Met de aanschaf van de PIA-tool ontstaat een meer structureel proces om privacy te borgen. Dit zal er ook voor zorgen dat de gepubliceerde informatie op basis van de PDCA-cyclus steeds zal worden bijgewerkt. Op 26 mei heeft de kick-off van de SmartPIA tool plaatsgevonden. Hiermee is het implementatietraject begonnen.
2 **Toegankelijkheid informatie:** dit omvat het tijdig, begrijpelijk en gemakkelijk, in duidelijke en eenvoudige taal verstrekken dan wel ontsluiten of beschikbaar maken van relevante informatie over verwerkingen van persoonsgegevens aan betrokkenen of belanghebbenden.	
Onderbouwing kwaliteitsniveau: 3	Voor rechtszoekenden en professionals moet het eenvoudig zijn om informatie te vinden over de wijze waarop de Rechtspraak omgaat met persoonsgegevens. Uit aandachtspunt 6 van de KPI Privacy Administratie is gebleken dat de Rechtspraak op twee verschillende plekken een privacyverklaring heeft gepubliceerd: - een algemene op rechtspraak.nl; en - een verklaring die aansluit bij de sollicitatieprocedure van de Rechtspraak. Mochten betrokkenen geïnteresseerd zijn in meer informatie over de Rechtspraak dan kunnen ze gebruikmaken van de verschillende communicatiekanalen die de Rechtspraak aanbiedt, zoals Facebook, Twitter, Instagram en Whatsapp. Daarnaast is het ook mogelijk om de FG te benaderen via functionarisgegevensbescherming@rechtspraak.nl.

Ambitieniveau: 4	Net als bij het vorige aandachtspunt zal de privacyverklaring door de nieuwe PIA-tooling continu worden geüpdatet. Verder kunnen ook vragen van betrokkenen aanleiding geven om de gepubliceerde informatie aan te passen.
3 Faciliteren uitoefenen privacy rechten door betrokkenen Transparantie gaat over de eenvoud waarop betrokkenen gebruik kunnen maken van hun privacy rechten	
Onderbouwing kwaliteitsniveau: 5	De privacywet- en regelgeving bieden rechtszoekenden en professionals de mogelijkheid om bepaalde rechten uit te oefenen. Het gaat dan bijvoorbeeld om recht op inzage, het recht van rectificatie en het recht om vergeten te worden. Om deze rechten te faciliteren is op rechtspraak.nl/privacy een procedure gepubliceerd hoe betrokkenen van hun rechten gebruik kunnen maken. Voor interne betrokkenen is het een en andere gepubliceerd op Intro. De procedures zijn ingevoerd binnen de Rechtspraak. Tijdens de implementatie is het volgende gerealiseerd: • Procedurebeschrijvingen en modelbrieven zijn aan gerechten en diensten ter beschikking gesteld door het AVG-projectteam van het Bureau Raad; • Gerechten en diensten zijn geïnformeerd over de procedure tijdens een aparte themamiddag; • Gerechten hebben een eigen coördinator informatieverzoeken die bereikbaar is Bij inwerkingtreding van de AVG werden de gerechten en diensten door de landelijk coördinator informatieverzoeken ondersteund bij het afhandelen van privacyverzoeken van betrokkenen. Al snel bleek dat de gerechten in staat waren de vragen zelf af te handelen. Vanwege een gebrek aan meerwaarde is de rol nu niet meer ingevuld. Eventuele vragen kunnen gerechten altijd stellen via [redacted]@rechtspraak.nl.
Ambitieniveau: -	Er zijn geen signalen dat er op dit punt op korte termijn nog acties ondernomen dienen te worden.

6. Privacy by design (PbD) en Default

Met Privacy by design wordt inzicht gegeven in de mate waarin rekening wordt gehouden met het kwaliteitsaspect privacy als aandachtspunt bij het ontwikkelen van nieuwe (werk)processen, informatiesystemen en/of beleid of wetgeving. Met privacy by default wordt beoogd (werk)processen, informatiesystemen en/of beleid te leveren die standaard uitgaan van de minst inbreukmakende gegevensverwerking.

De focus van de KPI PbD ligt daarmee bij het borgen van de belangenbescherming van de betrokkene waar persoonsgegevens van worden verwerkt.

De KPI Privacy by design en privacy by default bestaat uit **drie** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

<table>
<tr><td colspan="2">1 Privacy wordt meegenomen in ontwerpfase: PbD omvat het vroegtijdig bij en gedurende de doorlooptijd van nieuwe ontwikkelingen aandacht schenken aan de privacy aandachtsgebieden</td></tr>
<tr><td>Onderbouwing kwaliteitsniveau: 2</td><td>Ten aanzien van privacy in de ontwerpfase is een onderscheid te maken tussen:
- ontwikkelingen bij IVO;
- ontwikkelingen bij gerechten en andere diensten.

IVO
De meeste IT-ontwikkelingen vinden plaats bij IVO Rechtspraak. Voor zover er lokale ontwikkelingen zijn, zal privacy ad hoc aandacht krijgen in de ontwerpfase.

Tegelijkertijd wordt bij IVO privacy by design geïmplementeerd in de ontwikkelprocedures. Bij steeds meer ontwikkelingen wordt privacy by design gebruikt, maar een structurele aanpakt waarbij privacy daadwerkelijk vanaf het begin betrokken is, is nog in ontwikkeling. Hiervoor wordt samengewerkt met de ontwikkelteams. Daarnaast werkt de CISO/Teamleider SP&K aan een verbeterplan en een checklist Security & privacy.

Met terugwerkende kracht worden ook de oude IT-systemen AVG-compliant gemaakt (hierover meer onder aandachtspunt 2 van deze KPI).

Andere gerechten en diensten
Het principe van PbD is bij de gerechten en andere gerechten groeiende. Voor gerechten en diensten is het steeds duidelijk dat ze met de privacywet- en regelgeving aan de slag moeten. Daarvoor wordt dan ook steeds meer tijd vrijgemaakt. Enkele voorbeelden hiervan zijn:
- bij Rb Midden-Nederland is een medewerkster actief die de verwerkingen inventariseert en bepaalt of er een PIA moet worden uitgevoerd.
- Rb Gelderland, Rb Noord-Nederland en het Hof Arnhem-Leeuwarden gaan gezamenlijk een fulltime privacy officer werven die privacy binnen deze locaties verder gaat borgen. Daarnaast wordt ook een privacycoördinator door Rechtbank Oost-Brabant en Hof ’s-Hertogenbosch geworven.
- SSR en LSR hebben acties ondernomen om privacy verder te gaan borgen.
- Binnen het Bureau Raad en IVO Rechtspraak groeit de bewustwording t.a.v. privacy en de verplichtingen die dit met zich meebrengt.</td></tr>
</table>

	Ondanks dat privacywet- en regelgeving nog niet optimaal is geborgd, vallen er geen (grote) steken. Diensten en IT-producten worden via de inkoopafdeling van het LDCR of IVO aangeschaft. Bij de inkoopafdelingen van deze diensten zijn procedures ontwikkeld om privacy te borgen door een PIA uit te voeren en, voor zover nodig, door verwerkersovereenkomsten af te sluiten. Hierdoor wordt bij het aanbesteden van een nieuwe lokale dienst of ontwikkeling de privacy toch op een vroeg stadium in de aanschaf meegenomen. Daarnaast weten de meeste gerechten en diensten steeds beter het Bureau te vinden voor advies op maat. De beleidsmedewerker privacy & informatiebeveiliging zal hieraan blijven bijdragen.
Ambitieniveau: 3	De gerechten en de landelijke diensten moeten nog groeien in het toepassen van privacy by design. Er zijn ontwikkelingen, maar deze zorgen er nog niet voor dat privacy vanaf het begin al in scope is. Verder ontbreekt nog een cyclische werkwijze waarbij: 1) privacyrisico's vanaf dag één in kaart worden gebracht, 2) de maatregelen ter mitigatie van de risico's tijdens de ontwikkeling worden geïmplementeerd, 3) de maatregelen in het register van verwerkingsactiviteiten worden opgenomen en 4) periodiek wordt op de effectiviteit van de maatregelen gecontroleerd. Dit laatste kan leiden tot eventuele aanpassingen. . Hiervoor moeten de volgende acties worden ontplooid: - Verder implementeren van privacy by design bij IVO Rechtspraak en gerechten door o.a. het uitvoeren van PIA's en het bijwerken van het register van verwerkingsactiviteiten (IVO/beleidsmedewerker privacy & informatiebeveiliging; geen einddatum).
2 Afwegingen in het kader van beoordeling passende maatregelen PbD betekent het bij ontwikkelingstrajecten gestructureerd aandacht geven aan de beoordeling van wat passend is bij de aard, omvang, context en doel van de verwerking en ook anderszins proportioneel is (bijvoorbeeld kostentechnisch) dan wel subsidiair (kan het verwerken ook op een andere wijze, met minder risico's voor betrokkenen).	
Onderbouwing kwaliteitsniveau: 2	Artikel 32 van de AVG bepaalt dat persoonsgegevens op een passende manier moeten worden beveiligd. Dit betekent dat rekening moet worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. **Algemeen oordeel** Bij het merendeel van de verwerkingen zijn de maatregelen in kaart gebracht en geïmplementeerd. Er is echter nog werk dat opgepakt en gestructureerd moet worden uitgevoerd. Ter bespreking hiervan wordt een onderscheid gemaakt in: rubricering, bewaartermijnen, het wegwerken van auditbevindingen, het project AVG en autorisatiebeheer. Uiteindelijk wordt afgesloten met de kwaliteitsscore. **Rubricering** Rubriceren is het labelen van data op basis van de vertrouwelijkheid. Naar aanleiding van de collegiale toets is geconstateerd dat rubricering van

	datalekgevoelige informatie onvoldoende gebeurt. Om dit probleem op te lossen zijn er drie paden opgezet: - Aan de gerechtsbesturen is geadviseerd dat ze hun verantwoordelijkheid moeten nemen inzake het rubriceren van analoge informatie. - Door een team van medewerkers van IVO en het bureau Raad is een voorstel gemaakt voor een nieuw rubriceringskader dat de BIO volgt. In het nieuwe kader wordt naast 'vertrouwelijkheid' ook ingegaan op integriteit, beschikbaarheid en privacy. Het voorstel wordt verder gedeeld, besproken en eventueel aangepast. **Bewaartermijnen** Voor de Rechtspraak zijn de bewaartermijnen vastgelegd in zogenoemde 'Basis Selectie Documenten' (BSD). Deze zijn: - Het BSD Rechtelijke macht (geactualiseerd januari 2021): https://www.nationaalarchief.nl/archiveren/kennisbank/primair-proces-van-de-rechtspraak-selectielijst-voor-de-waardering-van-alle - Het BSD Bedrijfsvoering Rechtspraak (inclusief P-dossier): https://zoek.officielebekendmakingen.nl/stcrt-2018-23197.html Door het ministerie zijn nieuwe selectielijsten opgesteld en gepubliceerd. De Rechtspraak zal hierop moeten acteren en zijn eigen selectielijsten aanpassen om in lijn te lopen met het ministerie. Op basis van deze richtlijnen dienen de concrete bewaartermijnen per (onderdeel van een) systeem te worden opgetekend. In principe zijn de basisselectiedocumenten zowel voor papier als voor gegevens opgenomen in digitale systemen. Door de IVO-portefeuillehouder Generieke systemen/Bedrijfsvoering is, in afstemming met medewerkers van het Bureau Rvdr, een advies geformuleerd hoe bewaartermijnen uit de basisselectiedocumenten vertaald zouden kunnen worden naar systemen. Op dit moment is het beleid nagenoeg gereed. In eerste instantie was de verwachting dat de beleidslijn in 2020 was afgerond. Door ziekte is het werk echter blijven liggen. In april 2021 hebben de FG en de beleidsmedewerker privacy & informatiebeveiliging de nieuwe beleidslijn voorzien van feedback en teruggestuurd naar de IVO-portefeuillehouder. De portefeuillehouder heeft nog om een laatste reactie gevraagd van de FG. Hierna kan het door naar het SBO. **Het wegwerken van auditbevindingen** In 2019 heeft de actie gelopen om de auditbevindingen t.a.v. informatie-beveiliging op te schonen. Dit heeft geresulteerd dat in 2019 totaal 195 bevindingen zijn afgesloten. In 2020 zijn vervolgens 142 weggewerkt waardoor er nog 353 bevindingen open staan. Dit aantal is in 2021 teruggebracht tot 294 (peildatum 22 juni 2021). Hierbij moet rekening gehouden worden dat in 2020 en 2021 39 resp. 72 van deze openstaande bevindingen zijn geconstateerd. **Het Project AVG** Door IVO is een project gestart waarin systemenanalyses worden uitgevoerd om te bepalen welke aanpassingen gerealiseerd moeten worden om ze in lijn te brengen met de geldende privacywetgeving. Uiteindelijk is het dan aan de dienstenmanagers en portefeuillehouders om de aanpassingen in de systemen door te voeren.

	• Door het project is een faseplan opgesteld waarin gedetailleerder op de materie per systeemniveau wordt ingegaan. Dit document is op 1 september 2020 geaccordeerd door de stuurgroep van het project. • Voor het aanpassen van de systemen zullen nog een aantal beleidsmatige keuzes moeten worden gemaakt. Dit betreft o.a. t.a.v. bewaartermijnen (zie hierboven) en logging (zie hieronder). Om de maatregelen te kunnen implementeren is door het team architectuur van IVO Rechtspraak een statement opgesteld die in januari 2021 wordt geaccordeerd door de Design Authority van IVO Rechtspraak. Met dit statement is een fundament gelegd voor het ontwerp van o.a. logging. • In het geaccordeerde faseplan is een planning opgenomen voor het aanpassen van (primair proces)systemen. Iedere 6 maanden vindt een actualisatie van het faseplan plaatst. De eerste actualisatie wordt afgerond in in juli 2021. In eerste instantie is aangegeven dat de ambitie was om de wijzigingen begin 2022 doorgevoerd te hebben. Die planning was echter niet realistisch, omdat de verantwoordelijkheid voor het realiseren van de maatregelen buiten het project liggen. De deadline is nu 31 december 2022. • De aanpassingen ten aanzien van GPS worden onder leiding van het OM uitgevoerd. Het doel was om deze in maart 2021 te hebben afgerond. Het OM heeft echter besloten om GPS uit te faseren. Hierover is ook gesproken in de Raadsvergadering van 28 juli 2021. Het OM is vooral bezig met stabiliseren. De voorkeur ligt bij het gefaseerd en eigenstandig een eigen oplossing neerzetten voor de (kern)taken van Rechtspraak. • De AVG-analyses van geselecteerde systemen nadert zijn afronding en is naar verwachting uiterlijk september 2021 afgerond. • De IVO-directie is voornemens de (afwegingen m.b.t.) uitvoering van geadviseerde maatregelen uit de AVG-analyses centraal te beleggen bij een zogenaamde compliancytafel. Dit gremium is nog in oprichting, de organisatorische ophanging, de bezetting en het mandaat zijn nog niet definitief vastgesteld door de directie IVO. *Logging* De Wjsg, AVG en UAVG vereisen logging van gebruikershandelingen door de systemen. Door het ministerie van Justitie en Veiligheid is op 1 januari 2019 een KB gepubliceerd waarmee uitstel is verleend van de loggingsverplichting. Het interne loggingsbeleid is door IVO in de maak. De actie wordt gecoördineerd door team Kwaliteit vanuit de audit die is uitgevoerd door BKBO. Andere stakeholders (zoals privacy en security) worden betrokken in de verschillende reviewrondes. Verder wordt door IVO ook werkt aan een centrale voorziening voor logging. **Status aanpassing landelijk beheerde systemen** Begin oktober 2020 hebben de CIO Rechtspraak en de directeur Bureau Rvdr de onhaalbaarheid van de Wjsg-deadline naar de Raad voor de rechtspraak gesignaleerd. Door de CIO wordt bezien wat de precieze problematiek is en welke technische oplossingen er zijn. Ook zal bezien moeten worden wat e.e.a. betekent voor de investeringsplanning. Daarnaast zal bezien moeten worden welke preventieve, flankerende maatregelen genomen kunnen worden via bewustzijnsacties en via stringenter autorisatiebeheer. Het is aan de IVO directie en de onderliggende dienstenmanagers om de landelijk beheerde systemen in lijn met de privacywetgeving te brengen. De business (lees: dienstenmanagers) moet daarvoor een risicoanalyse uitvoeren o.b.v. de minimumnorm risicoanalyse IT. Op basis van de risicoanalyse kan een gewogen

	besluit genomen worden of een systeem wel of niet wordt aangepast. SP&K IVO heeft hiervoor een afwegingskader opgesteld. Dit afwegingskader ondersteunt bij het maken van een afweging of maatregelen worden doorgevoerd of dat het restrisico wordt geaccepteerd. Op dit moment voldoet Toezicht aan de eisen uit de privacywetgeving. Voor de andere systemen dragen het door team SP&K (IVO) opgestelde afwegingskader en de nieuw opgerichte compliancy tafel bij aan een afweging van de risico's. Hiervoor is geen planning beschikbaar gesteld. **Autorisatiebeheer** Het autorisatiebeleid is volgens de PwC-accountant niet op orde en de belangrijkste bevindingen waren[2]: • het ontbreken van (uniforme) procedurebeschrijvingen omtrent het toekennen, wijzigen en tijdig ontnemen van rechten in de primaire processystemen; • het ontbreken van inzicht in welke gebruikers over welke toegangsrechten beschikken in de primaire processystemen; • het ontbreken van een periodieke controle op de juistheid van de toegekende rechten aan gebruikers in de primaire processystemen. Om deze punten op te pakken lopen twee projecten: SIMS en informatierotonde. *SIMS* IVO is in 2019 een project gestart waarbij de rechtspraak aansluit op het systeem voor identiteitenmanagement van J&V (SIMS). Het project is op 17 mei 2021 décharge verleend. Er zijn enkele restpunten aan de service delivery management overgedragen. *Informatierotonde* Een andere project dat is opgestart na de bevindingen van de accountant, is het project autorisaties. Dit traject is samen opgepakt met functioneel beheer van IVO). Om inzicht voor elkaar te krijgen maakt het project gebruik van de informatierotonde, waarmee het mogelijk wordt om diverse gegevensbestanden van samenhang te voorzien en daaruit output te generen. Inmiddels is het project zover dat een groot aantal systemen (bijv. Civiel, Berber, Reis, Nias, Gps, Compas, etc.) in de informatierotonde zijn gekoppeld en dat enkele gerechten zijn voorzien van 'foutenlijsten' waarmee zij aan de slag kunnen. Met de publieke aandacht voor de problemen rondom de autorisaties bij de Politie, het UWV en recent ook de GGD komt ook voor de Rechtspraak de vraag op of dit bij ons wel goed geregeld is. Met het project autorisaties wordt hard gewerkt om hierin inzicht te verkrijgen. Daarna moet worden bepaald wie welke rechten mag hebben en of dit conflicten oplevert. Daarnaast merken de gerechten nu welke meerwaarde de informatierotonde heeft en komen er meermaals verzoeken om nog meer bestanden te koppelen. Na de opzet van een hoedanigheden platform wordt het mogelijk om ook de beveiligingsniveaus van informatie vast te leggen (classificatie of rubricering).
Ambitieniveau:5	Met het ambitieniveau sluit de Rechtspraak aan bij haar voorbeeldfunctie.

[2] PricewaterhouseCoopers Accountants N.V., Raad voor de rechtspraak Controle 2020 Rapportage interimbevindingen (Management Letter), 7 dec 2020.

	Hier wordt een onderscheid gemaakt in: algemeen, rubricering, bewaartermijnen, het wegwerken van auditbevindingen project AVG, en autorisatiebeheer. **Algemeen** • In de Raadsvergadering van 24 maart 2021 is afgesproken dat halverwege 2021 een overzicht moet zijn van mogelijke maatregelen en bijbehorende kosten. De Raad kan/moet dan keuzes gaan maken (directie IVO) • De portefeuillehouder in de Raad geeft aan dat er met betrekking tot het belang van privacy en informatiebeveiliging ook een structurele communicatie aanpak nodig is. Van belang is dat bij nieuwe projecten tijdig aandacht aan privacy en informatiebeveiliging wordt geschonken. **Rubriceren** Acties: • Bij de implementatie van de BIO wordt ook gewerkt aan een nieuw rubriceringskader. Dit rubriceringskader moet na afronding gedeeld worden met de gerechten, zodat zij dit kunnen gaan toepassen (beleidsmedewerker privacy & informatiebeveiliging en IVO; 1e kwartaal 2022). **Bewaartermijnen** Acties: • Voorleggen van de Beleidslijn bewaartermijnen aan het SBO (portefeuillehouder Generieke systemen/Bedrijfsvoering 3e kwartaal 2021). Hierna moeten de bewaartermijnen op basis van de notitie worden geïmplementeerd. **Het wegwerken van auditbevindingen** Acties: • Audit bevindingen t.a.v. beveiliging krijgen een hogere prioriteit en worden directer gemonitord (IVO, eind 2021). **Project AVG** De acties staan genoemd bij de bovenstaande onderbouwing van hey kwaliteitsniveau. **Autorisatiebeheer** De voortgangsstatus van het project informatierotonde wordt door de beleidsmedewerker privacy & informatiebeveiliging gevolgd. De PIA's voor het project zijn voorgelegd aan en positief beoordeeld door de FG. Vervolgens is de PIA vastgesteld door de directeur Bureau Raad.
3 Privacy by default Bij het beschermen van de persoonlijke levenssfeer van de betrokkene voorop staat bij ontwikkelkeuzen. Dit betekent dat altijd die optie wordt geselecteerd die in potentie de minste impact op de persoonlijke levenssfeer van een betrokkene zal hebben.	
Kwaliteitsniveau : 2	Het privacybewustzijn neemt steeds verder toe en medewerkers stellen steeds vaker vragen waarmee qua privacy rekening gehouden moet worden. Aan de andere kant gebeurt er ook nog veel onder de radar. De reden voor het gekozen kwaliteitsniveau is dat er wordt nagedacht over de verwerking met de minst grote impact, maar nog niet structureel.

	Tegelijkertijd wordt er ook nagedacht over een juiste borging, maar dit moet nog gerealiseerd worden. Hieraan zal de PIA-tool bijdragen.
Ambitieniveau: 3	De Rechtspraak beoogt het bewustwordingsniveau verder te vergroten en privacy by default structureel te borgen. De eerste stap is de PIA tool, zodat PIA's eenvoudiger kunnen worden uitgevoerd. De implementatie hiervan is op 26 mei 2021 gestart. Daarna kan het privacyproces verder worden geborgd. Hiervoor is geen concrete termijn te geven, omdat het afhankelijk is van het privacybewustzijn onder medewerkers.

7. Betrokken partijen

De KPI Betrokken partijen geeft inzicht in de wijze waarop organisatiegrens overschrijdend verkeer van persoonsgegevens is ingeregeld en persoonsgegevens buiten de beheersfeer van de verwerkingsverantwoordelijke en daarmee de organisatie raken.

Deze KPI kijkt op persoonsgegevensstromen van en naar betrokken partijen in verwerkingen. De onderbouwing van de rechtmatigheid van dit verwerken is een aspect waar de verwerkingsverantwoordelijke zich over dient uit te spreken en zijn maatregelenmix op moet inregelen. Het documenteren hiervan vindt plaats in het register van verwerkingsactiviteiten conform en langs de vereisten van art. 30 AVG.

Bij dit onderdeel is het van belang onderscheid te maken tussen:

- Een verwerkingsverantwoordelijke: stelt het doel (waarom?) en middelen (hoe?) vast van een verwerking.
- Een (sub)verwerker: een andere juridische entiteit die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke(n).

Uit het voorgaande kunnen dan drie soorten relaties worden onderscheiden:

- Verwerkingsverantwoordelijke – verwerker: de verwerkingsverantwoordelijk besteedt de verwerkingen uit aan een andere juridische entiteit. In dit geval moet een verwerkingsovereenkomst worden afgesloten.
- Twee verwerkingsverantwoordelijken: Een verwerkingsverantwoordelijke deelt gegevens met een partij die zelf doel en/of de middelen bepaald voor de verwerking. Een voorbeeld hiervan is het uitvoeren van een onderzoek. In dit geval moeten privacy afspraken worden afgesloten.
- Gezamenlijk verwerkingsverantwoordelijken: twee partijen stellen gezamenlijk het doel en de middelen voor de verwerking vast. In dit geval moeten privacy afspraken worden afgesloten.

Uit de PIA blijkt van welke relatie sprake is en dus welke soort overeenkomst is vereist.

De KPI Betrokken partijen bestaat uit **vier** aandachtsgebieden die hieronder verder worden uitgewerkt. Per aandachtsgebied wordt een korte beschrijving gegeven wat het inhoudt.

<table>
<tr><td colspan="2">1 Afspraken maken en overeenkomsten sluiten met gebruik van modellen: de taken die een verwerkersverantwoordelijke en een verwerker in kader van de gegevensuitwisseling over en weer hebben worden in het kader van de AVG en de Wjsg vormgegeven door vastlegging van afspraken in (bilaterale of multilaterale) afsprakenkaders en verwerkersovereenkomsten.</td></tr>
<tr><td>Onderbouwing kwaliteitsniveau: 4</td><td>Bij dit onderwerp wordt een onderscheid gemaakt tussen:
• De veelal landelijke contracten afgesloten door IVO
• De contracten afgesloten door de individuele gerechten en diensten

IVO
Het gaat hier om het afsluiten van privacyafspraken of verwerkersovereenkomsten voor systemen die landelijk worden gebruikt. De resterende verwerkersovereenkomsten worden in orde gemaakt. Er dienen nog voor enkele diensten verwerkersovereenkomsten te worden getekend. Daarbij dient te worden opgemerkt dat voor sommige diensten gezamenlijk met andere organisaties een verwerkersovereenkomst moet worden opgesteld. Denk hierbij aan grote IT- leveranciers als Microsoft, Adobe en Citrix. Er zijn reminders verstuurd, maar dit heeft nog niet tot wezenlijke vooruitgangen gezorgd.

Gerechten
Uit de beveiligingsbenchmark van gerechten 2019 van Motivaction d.d. 29 juli blijkt dat organisaties die te maken hebben met “verwerkers” bijna allemaal een verwerkersovereenkomst met externe partijen hebben. Dit is alleen niet het geval bij de Rechtbank Rotterdam, omdat daarvan geen statusupdate is ontvangen. Bij acht van de twintig organisaties is dit niet van toepassing.</td></tr>
</table>

	In de KCD-uitvraag van maart 2021 is opnieuw uitgevraagd of gerechten verwerkersovereenkomsten hebben afgesloten waar nodig. Bij de meeste gerechten en diensten zijn de overeenkomsten afgesloten. Bij andere zijn er nog wat verbeterpunten.
Ambitieniveau: 5	De Rechtspraak heeft nog niet voor alle externe datadelingen privacy-afspraken of een verwerkersovereenkomst opgesteld. Wel heeft de Rechtspraak in beeld waarvoor nog overeenkomsten afgesloten moeten worden. Acties: • De beleidsmedewerker privacy & informatiebeveiliging neemt contact op met de beveiligingscoördinator om te ondersteunen in het opstellen van verwerkersovereenkomsten (beleidsmedewerker privacy & informatiebeveiliging, 4e kwartaal 2021). • Afsluiten verwerkersovereenkomsten door IVO (actie nog nader te bepalen).
2 **Documentatie onderlinge verhouding t.a.v. verwerking in keten- of andere samenwerking:** is er sprake van gezamenlijke verwerkingsverantwoordelijkheid, wat voorkomt als twee of meerdere partijen doel en middelen van verwerken bepalen, moeten ook de onderlinge verhoudingen tot die verwerking worden gedocumenteerd in de registers van verwerkingsactiviteiten en de (bilaterale of multilaterale) afsprakenkaders.	
Onderbouwing kwaliteitsniveau: 3	Samenwerkingsverbanden zorgen ervoor dat persoonsgegevens buiten de organisatiemuren worden verwerkt. Zoals uit de introductie van dit hoofdstuk blijkt, kunnen deze samenwerkingsverbanden zich op verschillende manieren uiten. Gezamenlijke verantwoordelijkheid komt vooral voor in de relatie tussen de Raad voor de rechtspraak en de gerechten. In deze relatie is de onderlinge verhouding vastgelegd in diverse governance documenten. Zo ook voor privacy. Verder zijn er weinig gevallen waarbij sprake is van gezamenlijke verwerkingsverantwoordelijkheid. Voor het opstellen van privacyafspraken en verwerkersovereenkomsten zijn procedures opgesteld door het LDCR en IVO.
Ambitieniveau: 3	Op dit moment zijn er geen signalen die nopen tot acties om het kwaliteitsniveau te verhogen.
3 **Doorgifte persoonsgegevens aan een derde land:** er moet duidelijkheid zijn welke waarborgen er zijn getroffen door de verwerkingsverantwoordelijke opdat het voor natuurlijke personen vereiste beschermingsniveau niet wordt ondermijnd.	
Onderbouwing kwaliteitsniveau: 4	Van doorgifte van persoonsgegevens aan een derde land is sprake wanneer persoonsgegevens buiten de Europese Economische Ruimte worden verwerkt. Denk hierbij aan het versturen of opslaan van persoonsgegevens in de Verenigde Staten. In dit kader zijn vier punten relevant. Ten eerste zijn er binnen de Rechtspraak 15 applicaties die persoonsgegevens buiten de Europese Economische Ruimte (EER) versturen. Door de vernietiging van het adequaatheidsbesluit (Privacy Shield) door het Hof van Justitie van de EU wordt op dit moment door de dienstenmanagers samen met SP&K IVO in kaart gebracht wat de impact daarvan is voor de Rechtspraak. Op basis van de resultaten moet worden bepaald of de Rechtspraak na het wegvallen van het US-EU Privacy Shield in control is. Hiervoor zijn o.a. de volgende vragen van belang: 1) Wat hebben we als Rechtspraak staan in Amerikaanse cloud of staat in EER maar heeft risico van doorgifte naar VS? 2) Wat is juridisch/technisch mogelijk/noodzakelijk om te regelen? In hoeverre zijn er antwoorden op dit vraagstuk (vanuit EDPB, AP, Privacyboard JenV, etc.)? 3) Welke maatregelen neemt (IVO) Rechtspraak?

	De uitkomsten hiervan worden aan het bestuur voorgelegd. Ten tweede is noemenswaardig de relatie met het Gemeenschappelijk Hof van Justitie van de Nederlandse Antillen. Op dit moment vinden nog geen gegevensuitwisselingen plaats tussen de Rechtspraak en het Gemeenschappelijk Hof. Er wordt wel in kaart gebracht welke mogelijkheden er zijn om het Gemeenschappelijk Hof gebruik te laten maken van verschillende faciliteiten die de Rechtspraak intern gebruikt. De privacyrisico's zijn hier duidelijk in beeld. Ten derde is het cloudbeleid op 12 juli 2021 vastgesteld door het PRO, nadat achtereenvolgens de S&I- board en de Raad op 2 februari 2021 resp. 17 februari 2021 akkoord waren. Het cloudbeleid van de Rechtspraak biedt kaders voor het gebruik van clouddiensten. Het cloudbeleid wordt verder uitgewerkt in andere documenten, zoals een control framework en een cloudstrategie. Het cloudbeleid zal periodiek geactualiseerd worden. Om de kaders en de kennis te structureren en te borgen is er een cloudregiegroep en een cloud competence centre opgericht. Tot slot is als gevolg van de Brexit het Verenigd Koninkrijk een derde land. In het verdrag tussen de EU en het VK is een regeling opgenomen om ervoor te zorgen dat het uitwisselen van persoonsgegevens mogelijk blijft. Op 28 juni 2021 zijn door de Europese Commissie twee adequaatheidsbeslissingen genomen voor uitwisseling van persoonsgegevens met het VK. Het gaat om een adequaatheidsbesluit om persoonsgegevens in het kader van de AVG en de Richtlijn gegevensbescherming opsporing en vervolging.[3]
Ambitieniveau: 5	Er worden nadere verwerkersovereenkomsten door IVO opgesteld voor de bestaande diensten in de Amerikaanse cloud. Nieuwe diensten die de cloud in willen moeten daarvoor eerst langs de cloudregiegroep om daarvoor goedkeuring te krijgen. Voor de nieuwe Amerikaanse clouddiensten geldt dat in de verwerkersovereenkomst rekening moet worden gehouden met de opheffing van het privacy shield. Hiervoor is de standaard verwerkersovereenkomst aangepast. Zowel bij bestaande Amerikaanse clouddiensten als nieuwe Amerikaanse clouddiensten zal voorts moeten worden bezien of (technische) maatregelen genomen moeten worden of zijn zoals encryptie. Er wordt rekening mee gehouden in het cloudbeleid. Verder zal ook rekening moet worden gehouden met de totstandkoming van het adequaatheidsbesluit voor doorgifte naar het VK. De huidige regeling verloopt op 1 juli. Mocht het adequaatheidsbesluit niet tijdig worden vastgesteld, dan moeten aanvullende maatregelen worden genomen. De eerste stap hierin is het inventariseren van de verwerkingen waar persoonsgegevens in het VK worden verwerkt.
4 **Borgen informatiepositie en uitoefening rechten betrokkenen:** voor betrokkenen dient het bestaan van meerdere partijen geen onderscheid op te leveren om zijn rechten als betrokkene te kunnen uitoefenen (het bij elke partij aan kunnen kloppen met vragen over de verwerking) maar ook hoe en door wie invulling wordt gegeven aan de informatieplicht van partijen.	
Onderbouwing kwaliteitsniveau: 3	Ook wanneer sprake is van een samenwerkingsrelatie (zie 2) moeten de rechten van betrokkenen worden gewaarborgd. Hierover wordt het een en ander in de verwerkersovereenkomsten, verwerkersafspraken of privacyafspraken worden vastgelegd. Artikel 8 van de ARBIT- en ARVODI- template bepaalt dat de wederpartij zal ondersteunen bij de uitvoering van de rechten van betrokkenen. In dezelfde template wordt steeds opgenomen wie de wederzijdse contactpersonen zijn.

[3] Adequacy decisions | European Commission (europa.eu), geraadpleegd 5 juli 2021

	Hiermee wordt de mogelijkheid van betrokkenen om de wettelijke rechten uit te oefenen gewaarborgd. Betrokkenen worden niet proactief geïnformeerd over de partijen waarmee de Rechtspraak overeenkomsten heeft afgesloten. Algemene informatie over partijen waarmee de Rechtspraak samenwerkt staat in de privacyverklaring op rechtspraak.nl/privacy.
Ambitieniveau: 3	Op dit moment heeft de Rechtspraak nog geen signalen om het kwaliteitsniveau te verhogen.

8. Overige onderwerpen

Bij de J&V-indicatoren werden nog enkele andere punten benoemd die relevant zijn om te blijven monitoren, maar geen plek hebben gekregen in de privacy management KPI's. In dit hoofdstuk worden die onderwerpen voor de volledigheid behandeld.

a. Coronacrisis

Naar aanleiding van de verspreiding van COVID-19 heeft het kabinet in maart 2020 verschillende maatregelen afgekondigd. Het gevolg van deze maatregelen is onder andere dat rechtbanken alleen nog open zijn voor urgente zaken en dat het verzuim om verschillende redenen is toegenomen.

COVID-19 noodzaakt de gerechten maatregelen te nemen om ervoor te zorgen dat de bedrijfsvoering zo veel mogelijk doorgaat. De privacywetgeving blijft ook in tijden van crisis gelden en het is van belang dat de gerechten bij het nemen van de maatregelen hieraan, ondanks de crisis, blijven voldoen.

Met de versoepeling van de maatregelen is het ook weer mogelijk voor de gerechten om langzaam meer zittingen te laten plaatsvinden. Hiervoor is het een en ander voorbereid door het CMT, SBO en het LOBRO. Zo krijgt ieder gerecht een eigen register. In dit register wordt zes weken lang bewaard wie als publiek aanwezig is geweest bij een zitting. Bij een eventuele besmetting van een aanwezig persoon kan de Rechtspraak bijdragen aan het contactonderzoek. Op dit proces is een PIA Light uitgevoerd die is voorgelegd aan het PRO.

Acties (beleidsmedewerker privacy & informatiebeveiliging/FG; doorlopend gedurende de coronacrisis):

1. welke verwerkingen naar aanleiding van COVID-19 extra plaatsvinden;
2. toetsen of de verwerkingen rechtmatig gebeuren;
3. de gerechten adviseren wanneer gegevens in meer of mindere mate onrechtmatig worden verwerkt;
4. waarborgen dat de verwerkingen na opheffing van de beperkingen worden gestopt.

b. Privacy en de openbare registers

De wetgever heeft de Rechtspraak verplicht verschillende openbare registers bij te houden. Denk aan het Huwelijksgoederenregister (HGR), het Insolventieregister (CIR) en het Curatele- en bewindsregister (CCBR). Hoewel de grondslag en het doel voor deze registers uit de wet voort, is het vanwege het openbare karakter van belang dat de verwerking in de registers voldoet aan wettelijke kaders. Gegevens van een failliete natuurlijke persoon of rechtspersoon moeten niet langer dan noodzakelijk vindbaar zijn in het insolventieregister. Hetzelfde geldt voor de nevenbetrekkingen van rechters in het bijbehorende register.

Op dit moment worden de registers die de Rechtspraak beheert in het licht van de huidige privacywet- en regelgeving opnieuw moeten worden bezien. Nu steeds meer (keten)partijen de gegevens uit deze registers willen raadplegen en ontsluiten. Per register wordt nagegaan hoe deze zich verhouden tot de AVG. Dit moet leiden tot een visie op registers, waarin tevens de term 'register' eenduidig en concreet wordt gemaakt.

In week 33 wordt dit besproken met de betrokken portefeuillehouder in de Raad. Daarna wordt het besluitvormingstraject gestart.

Deelbesluit 1 - Datalekken
Document 10

datum	18 februari 2021
datum overleg	16 februari 2021
aanwezig	Olav Welling, [redacted]
Afwezig	[redacted]

Verslag werkgroep privacy 16 februari 2020

1. Opening en mededelingen
   a. [redacted] is aangesloten, loopt stage bij bureau vanuit Erasmus Universiteit en probeert alle overleggen binnen de Rechtspraak vast te leggen die organisatie-overschrijdend zijn.
   b. [redacted] gaat in vervolg CIO-office vertegenwoordigen. Hij heeft compliance-portefeuille gekregen.

2. Verslag 10 november 2020
   Paar correcties van [redacted]
   - [redacted] en [redacted] staan in het verslag zowel bij aanwezig als bij afwezig.
   - [redacted] staat tweemaal bij afwezig, dus een keer teveel.
   Actie [redacted] correcties doorvoeren.

3. Actielijst
   Er staan twee punten op de agenda. Enerzijds taken, verantwoordelijkheden en bevoegdheden (volgt later deze meeting), anderzijds bericht aan de PG HR.
   Bericht aan PG HR: [redacted] geeft aan dat er ontwikkelingen zijn op dit terrein binnen JenV. We wachten het rijksbrede traject in deze af.

4. Landelijke informatieverzoeken
   Olav geeft aan dat hij begrepen heeft dat landelijke informatieverzoeken niet in behandeling worden genomen, tenzij de verzoeker een concreet verzoek doet. Gelijktijdig is er geen grond om een verzoek af te wijzen. Het voorstel is nu om deze landelijke verzoeken wel in behandeling te nemen. Eerst volgt dan een vraag om het te specificeren (indien nodig) en [redacted] kan de coördinatie oppakken als landelijk coördinator.
   Er wordt opgemerkt dat [redacted] het afgelopen jaar op verzoek van de AVG-stuurgroep bij de gerechten heeft opgevraagd welke typen verzoeken zijn binnengekomen, dat viel erg mee tot juli 2020. We spreken af dat de voorgestelde aanpak gevolgd gaat worden.

   [redacted] merkt op dat gedurende de PrivacyBoard gesproken is over schadevergoedingen bij datalekken. Er worden nimmer bedragen meer dan 500 euro uitgekeerd, dit is toegelicht door onder meer de IND.
   Olav geeft aan dat er een voorbeeld is van een situatie bij de Raad waarbij ten onrechte niet was geanonimiseerd, het betrof daarbij niet enkel persoonsgegevens maar ook het feit dat na de melding de gegevens nog lang op de website van de Rechtspraak waren blijven staan. Daar heeft JZ een handvat voor bedacht. Er is in dat specifieke geval wel meer dan 500 euro uitgekeerd.

5. Zesde borgingsplan

a. Oplevering zesde borgingsplan
Diverse collega's hebben input geleverd. [redacted] heeft zijn best gedaan om in de leesbaarheid van het geheel een slag te maken. Het borgingsplan is naar Herma gestuurd. In het begeleidend schrijven is aandacht besteed aan enkele zorgen en enkele goede ontwikkelingen. Omdat deze zorgen vooral op het IVO-domein betrekking hadden, is gelijktijdig de directie van IVO geïnformeerd. Daar is een reactie op gevolgd van Jan Willem, waar Olav op gereageerd heeft. Ten eerste is gesproken over de oplevering van de planning t.a.v. het privacyproof maken van de systemen. We hopen dat deze in maart 2021 gaat volgen. De tweede opmerking betreft het overstappen op de BIO: er is reeds twee jaar geen overzicht t.a.v. de risico's voor informatiebeveiliging (zoals de omgang met bevindingen uit audits) en de uitwerking van de BIO. Het derde punt betreft de implementatie van Teams, analoog eraan Zoom. Gelukkig is er een PIA gemaakt voor Skype for Business. Olav geeft aan dat er PIA's rijksbreed zijn gemaakt voor Teams, maar de toepassing op de infrastructuur bij de Rechtspraak en autorisaties moeten wel goed ingeregeld worden. Op het vlak van informatiebeveiliging moet nog het e.e.a. gecheckt worden. Olav verwacht dat Herma aan IVO een reactie heeft gevraagd / zal vragen op het borgingsplan.

b. Registers
[redacted] vraagt wat er onder landelijk register en lokale registers moet worden verstaan. Het gaat hierbij om de verwerkingsregisters. [redacted] geeft aan dat zij de registers van de Rechtspraak heeft besproken met [redacted] **Actiepunt:** [redacted] **en** [redacted]

c. [redacted]

d. Meeting 15 februari
Verder geeft [redacted] aan dat op 15 februari een meeting heeft plaatsgevonden met diverse security professionals van enkele ketenpartners en de Rechtspraak. Hierbij waren vanuit onze organisatie een viertal collega's aanwezig. Het was een constructieve bijeenkomst waarbij gesproken is over de gevolgen van Teams, Webex etc. in relatie tot informatiebeveiliging. Hier is ook stilgestaan bij het primair proces.
Olav schetst zijn beeld bij de implementatie bij de Rechtspraak, deze zal allereerst zien op bedrijfsvoering, vervolgens op samenwerking en dan volgt mogelijk het primair proces. Er wordt voor het primair proces eerst gekeken naar een andere oplossing.
[redacted] geeft aan dat per type proces zal worden gekeken naar het gebruik van de tool, waarna de uitrol volgt. Voor Teams is gekozen voor de videochat en de presence-

functionaliteit in beginsel. Bij een select aantal organisatieonderdelen is ingestoken op een testfase, het gaat om IVO Rechtspraak, Bureau Raad en de rechtbank Overijssel. Bij deze locaties zal de samenwerkingsfunctionaliteit en bestanden delen uitgeschakeld zijn. De gerechten willen de tool graag gebruiken voor online zitten, maar het gaat nu om een beperkte pilot.
Olav geeft aan dat door het project Online Zitten wordt bekeken welke zaken geschikt zijn voor online zitten, waarna zal worden gekeken naar de eventuele implementatie. Eerst moet duidelijkheid worden verkregen over het soort zittingen, ook voor de periode na corona. Soms is daar wetgeving voor nodig. De ondersteuning voor dit project wordt verzorgd door [redacted].
[redacted] heeft een vraag over cloud in relatie tot de videoconferencetool 5.2 [redacted]

6. Bewaartermijnen
[redacted] geeft aan dat [redacted] enige tijd geleden een document over bewaartermijnen heeft opgesteld. Daar heeft het SBO op gereageerd halverwege 2020. De vraag is nu hoe we verder gaan. [redacted] heeft aangegeven dat het goed is om [redacted] hierbij te betrekken. Vanuit IVO is behoefte aan beleid op dit punt.
Olav geeft aan dat [redacted] bezig is met (de aanpassing van) een stuk over bewaartermijnen, dit ligt bij de AVG-werkgroep. [redacted] zou contact op kunnen nemen hierover met [redacted]. Idee achter het stuk dat eerder is gemaakt door [redacted] was het stellen van bewaartermijnen in plaats van een vergelijking en analogie te trekken met het papier. Dit, omdat er zoveel verschillende termijnen bestaan.
[redacted] gaat contact opnemen met [redacted] om te vragen wat de stand van zaken is v.w.b. bewaartermijnen. Zij kan ook verwijzen naar de archivarissen.
Actiepunt: [redacted]

[redacted] deelt de handreiking digitaal vernietigen die beschikbaar is gesteld op de website van het Nationaal Archief.

[redacted] vraagt aan [redacted] in hoeverre er concrete bewaartermijnen zijn opgenomen in de PIA's. [redacted] geeft aan dat sommige bewaartermijnen vooruit zijn geschoven, anderen zijn geconcretiseerd maar daarbij is de vraag of ze gehaald worden.

7. Werkgroep AVG Recofa
In verband met de afwezigheid van [redacted] licht [redacted] dit punt enigszins toe. N.a.v. een kamervraag ontstond een vraag over het gebruik van het BSN binnen de Rechtspraak. Er kwamen enkele duveltjes uit doosjes toen bij de gerechten werd gevraagd naar het gebruik

van het BSN (onder meer kopieën van paspoorten). Toen is bedacht om een werkgroep AVG bij Recofa op te starten. Recofa heeft te maken met digitaal en papier, het is van alles wat. [redacted] zal gevraagd worden om dit punt te bespreken met [redacted]
Actiepunt: [redacted]

8. Addendum Privacy Governance Rechtspraak
Olav vraagt of het document ondertussen goed genoeg is. Als er tekstuele opmerkingen zijn kunnen deze naar [redacted] dan kan de BVA gevraagd worden het te wijzigen als zijnde een niet-significante wijziging op de bestaande normen. Het is uiterst zorgvuldig uitgewerkt ondertussen en er kan mogelijk nog wel wat verschuiven, maar het is goed om dit vast te stellen. Als basis is er ruimschoots voldoende naar gekeken. Iedereen is hiermee akkoord.

9. W.v.t.t.k. / Rondvraag
   a. Verwerkersovereenkomst
   Succeswensje eind 2020 v.w.b. mandatering na afstemming met de advocaat van JenV. We hebben de verwerkersovereenkomst verbeterd en aangepast aan de Rechtspraak. Inmiddels is ook binnen het Rijk een werkgroep gevormd die gaat kijken naar de aanpassing van de ARVODI verwerkersovereenkomst. Er is een verschil van visie in verband met de brokers die soms betrokken zijn bij verwerkersovereenkomsten, hierover lopen de gesprekken. [redacted] en [redacted] volgen de ontwikkelingen en, indien nodig, kan de verwerkersovereenkomst van de Rechtspraak hierop aangepast worden in de toekomst. Het document is met diverse collega's afgestemd en kan in gebruik worden genomen.
   5.2 [redacted]

   b. 5.1(2)h [redacted]

   c. Privacy Pro's
   [redacted] geeft aan dat de reeks van het tweewekelijks bijpraatmoment is afgerond en zal ervoor zorgen dat dit weer opgepakt en ingepland gaat worden. Dat is goed om te horen.

de Rechtspraak

Actiepunt: [redacted]

10. Sluiting
    Olav zal over een week of zes een overleg laten inplannen en bedankt iedereen voor de aanwezigheid.

Deelbesluit 1 - Datalekken
Document 11

datum	23 december 2021
datum overleg	22 december 2021
aanwezig	Olav Welling, [redacted]
Afwezig	[redacted]

Verslag werkgroep privacy 22 december 2021

0. AVG bij IVO: planning en aanpak (te gast: [redacted], portefeuillehouder bedrijfsvoering)
   [redacted] geeft een toelichting over de geschiedenis en de huidige status van de implementatie van de privacywet- en regelgeving (m.n. de AVG en Wjsg). Daarna geeft ze toelichting op de notitie die naar de leden van de werkgroep is verstuurd. In deze notitie wordt een overzicht gegeven van de huidige stand van zaken, de bijbehorende risico's en de plannen voor volgend jaar.

   De applicaties zijn verdeeld in twee lijsten: een lijst met applicaties die snel kunnen worden aangepast en een lijst waar meer afhankelijkheden zijn. Bij deze laatste lijst gaat het vooral om de primaire processystemen. Er wordt een project gestart om deze aan te passen. De portefeuillegroep gaat het coördineren. SP&K monitort de voortgang. Mochten er discussie ontstaan of als er prioriteiten worden gesteld dan gaan die naar de compliancytafel. Deze compliancytafel is bedoeld om af te stemmen waar een bepaalde vraag over het aanpassen van een systeem naartoe moet. De Compliancy tafel bepaalt waar risico's worden belegd om hierover te beslissen.

   Met het oog op de historie geeft Olav aan dat we vaak de vraag krijgen of we compliant zijn. Voorheen gaven we de reactie dat we wel compliant waren, maar wel in control. Tegenwoordig geven we aan dat we ook niet in control zijn, omdat we niet weten wanneer de systemen worden aangepast. De laatste status geven we door sinds medio vorig jaar. Het is wel de bedoeling dat we binnenkort duidelijkheid hebben over de planning. De toegestuurde notitie is een goede eerste stap en er ligt ook het een en ander onder. Hierbij is van belang om te weten dat we altijd al rekening hielden met systemen die we niet zouden aanpassen, omdat de baten minder zouden zijn dan de kosten. Evenwel moet het besluit om het juiste niveau worden genomen.

   Opmerkingen kunnen tijdens het overleg worden gemaakt of na het overleg naar [redacted] worden gestuurd. Olav geeft aan dat hij en [redacted] een separate reactie naar [redacted] zullen sturen. Jan Willem is op de hoogte van de bespreking in de werkgroep privacy.

   Op verzoek van [redacted] geeft [redacted] aan dat autorisatie en logging volgend jaar (deze laatste in projectvorm) worden opgepakt.

Aanvullend vraag Olav hoe lang nodig is om duidelijk te krijgen wanneer systemen geactualiseerd worden of niet. [redacted] verwacht binnen twee weken meer duidelijkheid te krijgen van de SDM'ers.

5.2 [redacted]

Een ander relevant punt is of bestuurders de risico-inschatting van IV-organisatie delen. Het is dan ook van belang dat de Raad en vertegenwoordigers van de gerechten worden betrokken.

Olav vraagt zich tot slot af waarom de CISO wel en de FG/CPO geen onderdeel uitmaakt van de compliancy tafel. Volgens [redacted] is dit geen bewuste keuze geweest. [redacted] gaat ervan uit dat dat wordt aangevuld als ze de conceptversie deelt.

[redacted] stelt verder twee vragen:
- geeft het overzicht van systemen inzicht in welke onderdelen van de organisatie een raakvlak hebben met de systemen. [redacted] zegt dat de notitie aangeeft wat er moet gebeuren, door wie de acties moeten gebeuren en wat de kosten zijn.
- zijn de gevolgen van de aanpassingen duidelijk voor de gebruikers? [redacted] geeft aan dat gerechten zelf hun autorisaties moeten (laten) aanpassen. IVO helpt met groepen autorisaties.

[redacted] geeft nog aan dat – net als Olav aangeeft – de business moet zijn aangehaakt. 5.2 [redacted] geeft aan dit mee te nemen. 5.2 [redacted]

1. Opening/mededelingen
    a. KPI privacymanagement ([redacted])
    [redacted] geeft aan dat onlangs de nieuwe privacymanagement KPI's in de CIO Raad zijn besproken. Deze aangepaste KPI's gebruikt [redacted] voor de herijking van het borgingsplan begin volgend jaar. Op termijn wordt verwacht dat de KPI's nog zullen wijzigingen, omdat het gaat om een groeidocument.
    [redacted] vult na een vraag van Olav aan dat de KPI's niet veel verschillen ten opzichte van de eerste versie. Enkele artikelen zijn aangepast.

    Verder geeft [redacted] nog aan dat in de stukken voor de CIO Raad was opgenomen dat door JenV organisaties een volwassenheidsniveau van 3 nagestreefd moest worden. Aan [redacted] is toen meegegeven dat de Rechtspraak zelf het ambitieniveau bepaald. [redacted] en Olav zullen nog met elkaar bespreken of de kwaliteits- en ambitieniveaus ditmaal bestuurlijk goedgekeurd gaan worden.

2. Vaststellen verslag 25 oktober 2021
    Geen wijzigingen.

3. Acties
    a. Terugkoppeling livestreaming ([redacted])
    [redacted] geeft met [redacted] gesproken te hebben over de dienst livestreaming. Nadat [redacted] in 2020 met [redacted] heeft gesproken over het moment van uitvoering, waarbij [redacted] heeft aangegeven hiertoe bereid te zijn, is hem gevraagd hierbij te helpen. 5.2 [redacted]
    Later werd in het overleg aangegeven dat deze PIA als proef met SmartPIA kan worden uitgevoerd.

4. SmartPIA ([redacted])
    SmartPIA voor de Rechtspraak is voor 90% ingericht. [redacted] verwacht dat we in de tweede week van januari aan de slag kunnen met de basisinrichting. Die basisinrichting bestaat uit 3 vragenlijsten: een quickscan privacy, een vragenlijst register van verwerkingsactiviteiten en een FG-advies.
    Tijdens de implementatie van SmartPIA zijn we tegen verschillende punten aangelopen waarnaar nader onderzoek moest gebeuren. Daarnaast hebben er diversie sessies plaatsgevonden om de werking van SmartPIA te testen en te vergelijken met de papieren werkwijze. Dankzij SmartPIA is het mogelijk dat PIA's concreter, duidelijker en volledige worden. Tegelijkertijd is er minder tekst nodig dan op dit moment gebruikelijk is. Een ander punt is dat rollen en verantwoordelijkheid binnen het PIA-proces herzien moeten worden.
    Actie: [redacted] stuurt de aanpassingsvoorstellen naar [redacted]

[redacted] streeft ernaar SmartPIA in januari beschikbaar te stellen. [redacted] heeft een analyse gemaakt en een presentatie voorbereid die hij op verschillende plekken gaat geven.
5.2 [redacted] Hopelijk staan de PIA's in Q1 2022 in het systeem.

In januari gaat [redacted] verder met de verdere uitrol. Hieronder valt ook het register. Daarvoor wordt de Smartdashboard alsnog uitgevraagd. Dat bleek nu nog niet ingekocht te zijn. Deze tool haalt geautomatiseerd het register naar voren.

5. Datalekken digitale postkamer ([redacted] is twee weken geleden benaderd door [redacted] om een presentatie over datalekken in de digitale postkamer te reviewen. In die presentatie staat dat dit jaar ruim 2000 datalekken hebben plaatsgevonden. Het gaat dan veelal om adresseringsfouten.
Een oplossing is beeld. Begin volgend jaar starten ze met een pilot en pas per 2023 zou deze landelijk beschikbaar worden gesteld. Het gaat dan om twee maatregelen:
   - Toevoegen van een direct reageren knop waardoor alle adresseringsgegevens naar het nieuwe bericht worden gekopieerd.
   - Voor nieuwe berichten wordt een waarschuwing toegevoegd als de opgegeven referentie niet overeenkomt met de geadresseerde.

   Het is niet duidelijk waarom de datalekken niet in Classbase staan. [redacted] geeft aan dat dit nog wordt onderzocht. Olav geeft aan dat hierover duidelijkheid moet komen, zodat dit meegenomen kan worden in het jaarverslag.

5.2 [redacted]

6. Status onderzoek bewaartermijnen persoonsgegevens niet-zaaksgebonden processen ([redacted] geeft aan dat in oktober is gestart om – in aanvulling op de beleidslijn van [redacted] – een beleidsstuk op te stellen dat helpt bij de verdere concretisering van bewaartermijnen in niet-zaaksgebonden processen en systemen. In dit kader zijn de bewaartermijnen nog vaak onduidelijk door een omvangrijke hoeveelheid afspraken dan wel onduidelijk afspraken.
   Considerati voert het onderzoek uit. Ze hebben informatie ontvangen en hebben met 10 collega's gesproken. Het conceptrapport wordt begin volgend jaar verwacht.

7. Zittingslijsten voor de Commissie Intercollegiale Toetsing ([redacted] geeft aan dat hij begin dit jaar door de Raad voor de Rechtsbijstand zijn benaderd. Naar aanleiding van dat contact is er een PIA uitgevoerd op het proces rondom de Commissie Intercollegiale Toetsing dat bij enkele rechtbanken plaatsvindt.

   Betrokkenheid vanuit de vakinhoud is gewenst. Daarom vraagt [redacted] zich af hoe zij het beste betrokken kunnen worden. Olav geeft aan dat de expertgroep vreemdelingen van het LOV het beste kan worden benaderd. Hiervoor kan [redacted] contact opnemen met [redacted] Zij is waarschijnlijk op de hoogte van de collega die hierbij kan worden betrokken.

8. Rondvraag
   [redacted] geeft aan dat in de CIO Raad is aangekondigd dat een evaluatie van het JenV datalek gaat plaatsvinden. [redacted] vraagt of wij nog input willen leveren. Dit lijkt Olav wel gewenst. [redacted] stuurt de informatie die hij vanuit de CIO Raad heeft ontvangen naar [redacted] zodat hij kan bezien of het zinvol is om te delen.

   Olav geeft naar aanleiding van de vraag van [redacted] nog extra toelichting over gebeurtenissen op dit gebied. 5.2 [redacted]

9. Sluiting
   Olav vraagt aan [redacted] om een volgend overleg te plannen voor de tweede helft van februari. Op de agenda staat dan in ieder geval: Smartpia, borgingsplan en de notitie aanpak AVG/Wjsg.

Deelbesluit 1 - Datalekken
Document 12

datum	
datum overleg	16 februari 2022
aanwezig	Olav Welling, [redacted]
Afwezig	[redacted]

Verslag werkgroep privacy 16 februari 2022

1. Opening/mededelingen
   Er zijn verschillende nieuwe privacycollega's aanwezig: [redacted] (beveiligings- en veiligheidscoördinator rechtbank Overijssel), [redacted] (functionaris privacy bij IVO Rechtspraak), [redacted] (loopt stage bij het privacyteam van IVO Rechtspraak) en [redacted] (functionaris privacy bij IVO Rechtspraak).

   Iedereen stelt zichzelf kort voor. Daarna licht Olav het doel van de werkgroep privacy kort toe.

   a. Onderzoek bewaartermijnen niet-zaaksgebonden systemen en processen ([redacted] ligt toe dat het onderzoek is afgerond en dat hij aan de slag gaat met de omzetting van het eindrapport in een beleidsstuk. Hierbij houdt hij rekening met de beleidslijn bewaartermijnen die onlangs in het SBO is besproken.

   b. Statusupdate notitie IVO Rechtspraak inz. AVG/Wjsg ([redacted]/Olav)
      Olav, [redacted] en [redacted] hebben op verzoek van Jan Willem feedback gegeven op de stand van zaken notitie AVG/Wjsg d.d. 1 februari 2022. Een aangepaste versie van deze notitie is besproken in de Raadsvergadering van 16 februari 2022. Olav geeft een terugkoppeling van hetgeen in die vergadering is besproken.

      In notitie van IVO Rechtspraak staat dat de Rechtspraak in control is. De notitie bevat echter geen planning. Dat is voor de Raad onvoldoende. De Raad wil inzicht krijgen in de planning en de risico's die de Rechtspraak loopt door bepaalde systemen niet of later te verbeteren. Op basis van de huidige versie kunnen zij niet bepalen hoe de Rechtspraak ervoor staat. Alle leden willen op de hoogte willen zijn van de risico's.

      In de vergadering is afgesproken dat een planning vóór 1 april in de Raad wordt besproken.

2. Vaststellen verslag 22 december 2021
   Geen inhoudelijke opmerkingen. [redacted] en Olav bespreken punt 7 buiten het overleg verder.

3. Acties
   a. Actualisatie PIA-proces door implementatie SmartPIA ([redacted]

[redacted] neemt hierover contact op met [redacted] Ze informeert [redacted] als het proces is bijgewerkt. Daarnaast laat [redacted] weten dat de reeds uitgevoerde PIA's niet in Q1 in SmartPIA zullen staan. Om alle bestaande PIA's in SmartPIA te zetten is meer tijd nodig, omdat de vragenset in SmartPIA anders is dan de vragenset voor de PIA. Iedere PIA moet in overleg met de SDM'er of proceseigenaar in SmartPIA worden geplaatst.

4. SmartPIA ([redacted])
[redacted] Geeft aan dat het project nog steeds conform planning verloopt. Op dit moment wordt een acceptatietest van de vragensets uitgevoerd. Deze test doet hij samen met het privacyteam. Als het privacyteam de vragensets accepteert, dan kunnen we bestaande PIA's gaan invoeren. Zoals door [redacted] reeds is aangegeven, zal dit langer duren dan oorspronkelijk gedacht.

   Vooralsnog kunnen de meeste vragen worden getackeld. Er zijn al belangrijke nieuwe lessen geleerd tijdens de pilot waardoor de kwaliteit van het systeem aanzienlijk is verbeterd. Op termijn wordt de kwaliteit van PIA's ook beter.

   Tot slot geeft [redacted] aan dat het dashboard voor het register van verwerkingsactiviteiten beschikbaar is.

5. Uitwisselmap G:-schijf (privacyteam IVO)
[redacted] en [redacted] introduceren het probleem. Onlangs is geconstateerd dat vertrouwelijke stukken onversleuteld in de uitwisselmap op de G-schijf stonden. Hierdoor kon medewerker kennis nemen van de stukken. [redacted] en [redacted] hebben actie ondernomen door contact op te nemen met de beveiligingscoördinatoren van de gerechten die vertrouwelijke stukken onversleuteld op de G-schijf hadden geplaatst. Zij zijn verzocht de informatie te laten verwijderen en een datalekmelding aan te maken.

   Verder is het van belang dat we bepalen hoe we in het algemeen omgaan met de uitwisselschijf. Uit de verkennende probleemanalyse blijkt dat het gaat om meerdere problemen. Derhalve zijn meerdere oplossingen nodig om de uitwisselschijf op de juiste wijze te gebruiken. Tijdens het afgesproken wordt afgesproken dat [redacted] [redacted] en [redacted] een probleembeschrijving opstellen. Daarna kunnen we kijken hoe we het probleem oplossen en waar we het probleem plaatsen in de prioritering. [redacted] denkt graag mee, omdat ze ervaring heeft met het oplossen van dit soort problemen.

6. Opendatarichtlijn in relatie tot Meer en verantwoord publiceren ([redacted]
[redacted] geeft aan dat het doel van het programma is om 75% van de uitspraken te gaan publiceren. Meer publicaties betekent in absolute getallen ook meer anonimiseringsfouten. Om grootverbruikers over een anonimiseringsfout te kunnen informeren, wordt een registratie overwogen (in lijn met overweging 44 Opendatarichtlijn).

Hiermee kunnen grootverbruikers sneller de fout op hun site herstellen. Tegelijkertijd stelt een register de Rechtspraak in staat een klankbordgroep in te richten.

[redacted] geeft aan dat het gaat om een overweging gaat, dus niet om een vastgesteld artikel. Dat verandert het belang van de overweging. [redacted] geeft aan dat het nog geen zekerheid is dat er daadwerkelijk een register komt. Het programma is hierover nog in gesprek.

Aansluitend vraagt [redacted] hoe en wie men het privacyteam bij het programma wil betrekken. [redacted] geeft aan dat het programma nu nog in de verkennende fase is en dat de eerste contacten inzake wetgeving zijn gelegd. [redacted] zal worden betrokken als het programma uit de verkennende fase is.

7. Update borgingsplan en scoring kwaliteits- en ambitieniveaus ([redacted])
[redacted] geeft een toelichting ten aanzien van het geactualiseerde borgingsplan. Afgesproken wordt dat leden van de werkgroep voor 19 februari 2022 reageren ten aanzien van de voorgestelde kwaliteits- en ambitieniveaus. Daarna wordt het borgingsplan geagendeerd voor de Raadsvergadering. In de oplegnotitie wordt in ieder geval informatie gegeven ten aanzien van de ontwikkelingen sinds 1 feburari 2022 (peildatum borgingsplan).

8. Wetenschappelijk onderzoek en privacy ([redacted])
[redacted] geeft aan dat in 2021 20 externe onderzoeken zijn behandeld. Deze zijn niet meegenomen in de teling van het aantal PIA's in het jaarverslag van het Bureau Raad. Alle PIA's zijn voorzien van een FG-advies dat samen met het voorstel naar de LOV's is gegaan. De PIA's kosten veel tijd waardoor andere dingen blijven liggen.

[redacted] licht een voorbeeld toe dat recent veel tijd heeft gekost. Naar aanleiding van dat voorbeeld wordt samen met de andere FG's in de strafrechtketen besproken hoe we gezamenlijk een oplossing kunnen vinden voor verzoeken om informatie van externe partijen.

9. Terugkoppeling datalekken digitale postkamer ([redacted])
[redacted] deelt de terugkoppeling die recentelijk ook is gedeeld met de beveiligingscoördinatoren. Door twee beveiligingscoördinatoren is een vervolgonderzoek gestart. [redacted] zal aandacht vragen in het LOBRO voor dit onderwerp.

Wordt vervolgd.

10. Rondvraag
- [redacted] geeft aan te werken aan een visie op registers. De volgende stap is om het gesprek met het ministerie aan te gaan over de onderliggende wet- en regelgeving van de (openbare) registers die de Rechtspraak beheert. Een toets of de wet- en regelgeving nog in lijn is met de AVG is noodzakelijk. Binnenkort heeft ze een gesprek met de plv. CIO en SG van het betreffende departement.

- [redacted] heeft een viertal punten:
  - Er is een nieuwe FG bij de Hoge Raad, maar de oude FG blijft wel ondersteunen.
  - De Hoge Raad heeft de contactgegevens gevraagd van alle privacycoördinatoren van de Rechtspraak. Door diverse redenen is de inventarisatie nog niet rond. [redacted] constateert dat niet altijd duidelijkheid is wie als contactpersoon fungeert.
  - De herziening van de Wjsg en de Wpg is niet meegenomen in de financiën van de nieuwe minister. Hierdoor is niet duidelijk hoe het vervolg eruit gaat zien.
  - Op 6 mei vindt een overleg plaats over de herziening van Richtlijn 2016/680. Het ministerie van Justitie en Veiligheid heeft een visie aan de Europese Commissie verstrekt, maar de Rechtspraak was daar niet van op de hoogte en is ook niet benaderd. De deadline voor input vanuit de Rechtspraak is 21 februari 2022. Een eventuele reactie vanuit de Rechtspraak volgt gezien de korte termijn in de volgende ronde.
- [redacted] heeft twee punten:
  - De Autoriteit Persoonsgegevens heeft samen met de andere toezichthouders aangekondigd dat een onderzoek wordt gestart naar het gebruik van cloudoplossingen door publieke partijen. [redacted] is benieuwd of de Rechtspraak vanwege de beperkte toezichthoudende rol van de AP ook bij dit onderzoek betrokken zal worden. In het verleden is gebleken dat de AP niet weet hoe ze zich ten opzichte van de Rechtspraak moet positioneren.
  - [redacted] neemt met [redacted] contact op om de omvang van de werkgroep privacy te bespreken. Hoewel de interesse voor het overleg groot is, wordt ook geconstateerd dat het overleg een groot beslag legt op de beschikbaarheid van het privacyteam. Daarnaast is er ook veel overlap in de betreffende functies. Er wordt daarom een gekozen voor een vorm van vertegenwoordiging. Omvang werkgroep privacy
- [redacted] gaat nog in op het onderwerp testen met productiedata en testen in de productieomgeving. Er is een procedure en een format opgesteld om diensten te ondersteunen. Hoewel diensten periodiek gebruik maken van deze middelen om toestemming te krijgen, is tot op heden nog geen positief advies gegeven. Dit zorgt voor frustratie binnen de organisatie. Dit probleem is niet uniek voor de Rechtspraak, maar speelt ook bij andere organisaties.

  [redacted] gaat onderzoeken hoe andere organisaties hiermee omgaan en stelt op basis daarvan een voorstel op dat ze wil bespreken. Uiteindelijk moet dit leiden tot een advies (met opties) aan de directie van IVO Rechtspraak als beslissingsbevoegde.

11. Sluiting

Olav sluit de vergadering.

Deelbesluit 1 - Datalekken
Document 13

(8E) Borgingsplan Privacy Rechtspraak (peildatum 15 februari 2022)

Versie 1 maart 2022

Inhoud

Afkortingen

AVG	Algemene verordening gegevensbescherming (EU- verordening 2016/679)
ARBIT	Algemene Rijksinkoopvoorwaarden bij ICT-overeenkomsten
ARVODI	Algemene Rijksinkoopvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten
BVA	Beveiligingsautoriteit
BVC	Beveiligingscoördinator
BSD	Basis Selectie Document
CISO	Chief information security officer
CIO	Chief information officer
FG	Functionaris gegevensbescherming
HR(M)	Human Resource (Management)
IVO Rechtspraak	Informatievoorzieningsorganisaties Rechtspraak
JenV	Ministerie van Justitie en Veiligheid
KCD	Key Control Dashboard
KPI	Kritieke prestatie-indicatoren
LBVr	Landelijk Bureau Vakinhoud rechtspraak
LDCR	Landelijk Dienstencentrum Rechtspraak
(DB) LOBRO	(Dagelijks bestuur) Landelijk Overleg Beveiligingscoördinatoren Rechterlijke Organisatie
PbD	Privacy by Design
PDCA-cyclus	Plan-Do-Check-Act-cyclus
PGHR	Procureur-Generaal bij de Hoge Raad
PIA	Privacy Impact Assessment
PRO	Presidenten-Raad Overleg
Richtlijn	Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn 2016/680)
Rvdr	Raad voor de rechtspraak
SBO	Strategisch Bedrijfsvoeringsoverleg
SP&K	Security, Privacy & Kwaliteit
S&I-Board	Strategie en Innovatie board
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
Wjsg	Wet justitiële en strafvorderlijke gegevens

1. Inleiding

Aanleiding

Het uitgangspunt van de Rechtspraak is om altijd naar de letter en geest van de geldende privacywet- en regelgeving te handelen. Dit kader wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), Wet justitiële en strafvorderlijke gegevens (Wjsg) en het bijbehorende besluit (hierna: de privacywet- en regelgeving).

Voorafgaand aan de inwerkingtreding van de privacywet- en regelgeving is het Bureau Raad het Project AVG gestart om de privacywet- en regelgeving op gestructureerde wijze te implementeren en te borgen. Na de inwerkingtreding van de AVG op 25 mei 2018 is het project gestopt. De resterende werkzaamheden zijn in de lijn verder opgepakt.

Doel

Om inzicht te behouden in de nog openstaande punten, is het borgingsplan privacy opgesteld. Hierin staan de activiteiten die nog moeten worden ondernomen de privacywet- en regelgeving (verder) te implementeren en te borgen.

Herijking

Om het doel van het borgingsplan te volbrengen, wordt het plan halfjaarlijks herijkt. Hierdoor blijft het borgingsplan een actueel beeld geven van de werkzaamheden die ten aanzien van privacy nog moeten worden verricht. Daarbij wordt ook zo goed als mogelijk inzage gegeven in de planning per actie.

Nadat het eerste borgingsplan in januari 2019 is vastgesteld, is het onderhavige document de achtste versie.

KPI's

In dit document wordt de implementatie en borging van de privacywet- en regelgeving beschreven op basis van de kritieke prestatie-indicatoren (KPI's) die door het ministerie van Justitie en Veiligheid in het kader van privacymanagement zijn opgesteld. De Rechtspraak heeft naar aanleiding van de pilot die JenV-breed is uitgevoerd, gekozen dit instrumentarium te gebruiken om de borging van privacy op gestructureerde wijze intern te rapporteren.[1]

De privacymanagement KPI's blijven na de pilot continu in ontwikkeling. In deze versie van het borgingsplan is versie 1.0 (datum november 2021) van de KPI's gebruikt.

Leeswijzer

Het vervolg van het document is als volgt. In hoofdstuk 2 wordt een algemeen beeld gegeven over de implementatie en borging van de privacywet- en regelgeving binnen de Rechtspraak. In hoofdstuk 3 wordt ingegaan op hoe en door wie het borgingsplan wordt samengesteld. Vervolgens wordt in hoofdstuk 4 tot en met 7 op basis van de vier privacy management KPI's van JenV de status ten aanzien van privacy weergegeven. Tot slot worden in hoofdstuk 8 nog enkele onderwerpen behandeld die relevant zijn voor de Rechtspraak, maar niet passen in een van de KPI's.

[1] KPI 10 (Waarborgen van een passend beveiligingsniveau) is op basis van de ervaringen met de eerdere versies van de KPI's specifiek toegevoegd voor de Rechtspraak.

2. Beeld Rechtspraak

Er is al veel werk verzet, maar er is ook nog genoeg te doen. Om het algemeen beeld van de Rechtspraak uit te drukken wordt gebruik gemaakt van de termen: ‘in-control’ en ‘compliant’. Met dit eerste wordt bedoeld dat nog niet op alle onderdelen aan de geldende privacywet- en regelgeving wordt voldaan, maar dat wel duidelijk is wanneer hieraan voldaan wordt. Met dit tweede wordt bedoeld dat aan alle onderdelen van de privacywet- en regelgeving wordt voldaan en dat de onderdelen zijn geborgd. Hierbij moet de kanttekening gemaakt worden dat nooit sprake kan zijn van 100% compliancy. De stand van de techniek en de interne en externe omgeving veranderen dusdanig snel dat altijd ruimte is voor verbetering. Borgen staat daarom centraal.

Het Bureau BVA concludeert dat de Rechtspraak niet volledig in-control of compliant is met de geldende privacywet- en regelgeving. Dit komt door een onvolledig overzicht in het ICT-landschap en het gebrek aan een heldere planning om de informatievoorziening in lijn met de geldende privacywet- en regelgeving te brengen. Om in-control te komen zal de Rechtspraak ervoor moeten zorgen dat er een overzicht is waaruit blijkt welke systemen de Rechtspraak gebruikt en hoe de systemen gegevens verwerken. Tegelijkertijd moet er een eenduidige planning zijn om de systemen in de informatievoorziening in lijn te brengen met de privacywet- en regelgeving. Bij dit laatste bestaat de mogelijkheid om systemen, na een risicoafweging, niet meer aan te passen.

Verder wordt 2022 een belangrijk jaar t.a.v. privacy met het oog op de loggingsverplichting in strafsystemen. Op grond van artikel 63, tweede lid Richtlijn moeten de strafsystemen van de Rechtspraak die voor mei 2016 zijn ontwikkeld, voor 6 mei 2023 voldoen aan de loggingsverplichting. Deze verplichting houdt in dat de informatiesystemen van de Rechtspraak gebruikershandelingen moeten vastleggen. Er is een mogelijkheid om in uitzonderlijke omstandigheden de deadline te verlengen tot uiterlijk 6 mei 2026. De Rechtspraak heeft daarom tot doel om op 31 december 2022 aan de loggingsverplichting te voldoen. Is dat niet mogelijk, dan zijn er nog 5 maanden om verzoek tot verlening van de deadline in te dienen.

De Rechtspraak is bij de nakoming aan artikel 63, tweede lid Richtlijn deels afhankelijk van de keuzes die het OM maakt, omdat de Rechtspraak verschillende strafsystemen van het OM gebruikt. Desalniettemin heeft de Europese wetgever de loggingsverplichting bij de verwerkingsverantwoordelijke gelegd. De Rechtspraak is verwerkingsverantwoordelijk voor de gerechtelijke strafgegevens. Hierdoor blijft de Rechtspraak verantwoordelijk om ten aanzien van de gerechtelijke strafgegevens aan artikel 63, tweede lid Richtlijn te voldoen. Het gebruik van OM systemen maakt dat niet anders.

Het bovenstaande geldt echter niet voor de andere informatiesystemen van en andere verplichtingen voor de Rechtspraak. Hiervoor geldt per 25 mei 2018 een verplichting om passende waarborgen te treffen. Hieronder valt ook het bijhouden van gebruikershandelingen om misbruik te controleren.

3. Werkwijze en totstandkoming

Dit plan is ingedeeld conform de privacymanagement KPI's vanuit het ministerie van Justitie en Veiligheid (JenV). KPI worden verschillende aandachtspunten behandeld. Deze scoring vindt plaats op twee niveaus: het kwaliteitsniveau en het ambitieniveau. De scoringsniveau's gaan van 1 (laagst) t/m 5 (hoogst).

De KPI's zijn zodanig opgesteld dat bij niveau 1 al wordt voldaan aan de verplichtingen uit de privacywet- en regelgeving. Een goede borging van privacy vraagt van de Rechtspraak echter om verder te gaan dan het minimale en te kijken wel structurele verbeteringen kunnen worden doorgevoerd. Een organisatie kan daarom op basis van de niveaus welke ambities passend zijn.

Kwaliteitsniveau
Ieder aandachtspunt krijgt een score voor het kwaliteitsniveau dat past bij de huidige situatie. De score wordt onderbouwd aan de hand van voorbeelden (zoals bestaande afspraken, procedures, processen, diensten en producten). Hieruit moet de passendheid van het aangegeven kwaliteitsniveau blijken.

Ambitieniveau
In relatie tot het kwaliteitsniveau wordt aangegeven wat bij ieder aandachtspunt de ambitie van de Rechtspraak is. Hierbij wordt aangegeven welke acties nodig zijn om tot dat niveau te komen. Aan iedere actie wordt een actiehouder en een deadline gekoppeld, zodat periodiek de voortgang wordt vastgesteld. Tegelijkertijd zorgt een actie ervoor dat privacy wederom aandacht en prioriteit krijgt.

Overall-aanpak
Dit borgingsplan is opgesteld in opdracht van de Raad voor de rechtspraak. Opdrachtnemer is de directeur van het Bureau van de Raad voor de rechtspraak.

De uitvoering van de activiteiten wordt gecoördineerd door een werkgroep met daarin de volgende deelnemers:

- Functionaris gegevensbescherming
- Privacy officer IVO
- Functionarissen privacy IVO
- Teamleider security, privacy & kwaliteit IVO/ Chief Information Security Officer (CISO)
- Beleidsmedewerker privacy bureau Rvdr
- Lead adviseur IV-strategie en -beleid (CIO office)
- (senior)adviseurs Recht & ICT afdeling Strategie Bureau Rvdr

Agendalid: stafmedewerker Europees recht Landelijk Bureau Vakinhoud rechtspraak

De daadwerkelijke uitvoering van de activiteiten ligt bij een veel grotere groep medewerkers waarbij medewerkers op het terrein van informatiebeveiliging, service delivery, architectuur, applicatiebeheer, inkoop, portefeuillehouders en de lokale privacycoördinatoren bij de gerechten belangrijke partijen zijn.

Beperkingen
Het plan gaat niet in op de werkzaamheden van het Landelijk Bureau Vakinhoud rechtspraak (LBVr), waarbij het gaat om de werkzaamheden die liggen in het verlengde van het werk van de rechter. Hiervoor is de werkgroep AVG vakinhoud opgericht die bestaat uit experts vanuit de gerechten. Vanzelfsprekend is er wel samenwerking met en uitwisseling van kennis tussen het LBVr en de betrokkenen vanuit (de bedrijfsvoering van) de Rechtspraak.

De mate van implementatie en borging van privacy op lokaal niveau wordt bepaald op basis van de KCD-rapportage, de benchmark en de collegiale toets van het Bureau BVA. Daarnaast wordt gebruik gemaakt van signalen vanuit de gerechten.

4. Privacyadministratie

Privacyadministratie omvat alle KPI's voor de Rechtspraak die van belang zijn om te voldoen aan de verantwoordingsplicht uit de privacywet- en regelgeving. Aan de hand van de KPI's geeft de verwerkingsverantwoordelijke inzicht in de status quo van de wettelijk verplichte documentatieopbouw voor deze aandachtsgebieden (documentatieplicht) en laat zien wat er zoal op de rit is als onderbouwing voor de door de organisatie gehanteerde zorgvuldigheid in haar omgangsvormen met persoonsgegevens.

1. Privacybeleid	
Norm	De organisatie heeft doelstellingen en verantwoordelijkheden op het gebied van privacy neergelegd in een formeel vastgesteld privacybeleid.
Referentie	Artikel 24, eerste lid, artikel 5, tweede lid AVG Artikel 3 Wjsg[2]
Beoordeling	
Kwaliteitsniveau: 4	Het privacybeleid wordt in meerdere documenten op meerdere niveaus vormgegeven: - Strategisch niveau: o Strategisch plan privacy[3] o Beveiligingsbeleid voor de Rechtspraak 2019-2023 - Tactisch niveau: o Minimumnormen beveiliging en privacy o ICT-normenkader o Evt. intern beleid (bijv. Privacybeleid IVO) - Operationeel niveau: o Procesbeschrijvingen en best practices Het beleid wordt periodiek herijkt. Zo wordt het beveiligingsbeleid voor de Rechtspraak iedere vier jaar en de minimumnormen iedere twee jaar herzien. In 2022 worden de minimumnormen herzien en wordt gestart met het Beveiligingsbeleid voor de Rechtspraak 2023 – 2027. Hieronder wordt nog nader ingegaan op de implementatie van de baseline informatiebeveiliging overheid (BIO). De BIO heeft namelijk op verschillende punten geleid tot wijziging van beleidsstukken die relevant zijn voor de beveiliging van persoonsgegevens. **BIO** Nadat IVO Rechtspraak in januari 2020 is overgestapt op de BIO, hebben de gerechten en andere diensten ook besloten over te stappen naar de BIO. Om deze overstap te maken zijn vanuit het Bureau BVA op diverse punten aanpassingen in de beleidsstukken voorgesteld. Deze aanpassingen zijn op 22 november 2021 – na afstemming met IVO - door het SBO geaccordeerd. Onderdeel van de besluitvorming vormde de verdeling van de invulling van de normen. Verschillende normen zijn van dermate technische aard dat deze alleen door IVO kunnen worden uitgevoerd voor zover het gaat om systemen die door IVO worden beheerd. Tijdens de collegiale toets wordt gecontroleerd of IVO aan deze normen voldoet. Is dat het geval, dan geldt dat ook voor de gerechten. Voor zover het gaat om lokale applicaties, is het de taak van de gerechten om te controleren of die applicaties aan de betreffende BIO-normen voldoen.

[2] In de artikelen 51f en 51h Wjsg worden de genoemde Wjsg-artikelen van overeenkomstige toepassing verklaard op gerechtelijke strafgegevens.
[3] Vastgesteld door het PRO in september 2017.

	IVO werkt aan de verdere concretisering van de BIO-normen. De controls in de BIO zijn namelijk op een hoog abstractieniveau. De IT-normenkaders moeten deze controls verduidelijken en aanvullen met andere relevante normen. De organisatie moet deze kaders verplicht volgen. Eventuele handreikingen zijn niet verplicht. Hiermee krijgt het informatiebeveiligingsbeleid van IVO (en daarmee de Rechtspraak als geheel) drie lagen: de controls in de BIO, de IT-normenkaders en eventuele handreikingen.
Ambitieniveau: 5	De Rechtspraak scoort hoog op deze KPI. Privacy is onderdeel van het Integrale veiligheids- en beveiligingsbeleid en wordt daarom herzien in dezelfde cadans als de andere beleidsstukken. Om het hoogste ambitieniveau te halen moet uit het privacybeleid blijken dat privacy een kernwaarde is van de organisatie. De Rechtspraak kan op dit onderwerp verbeteren doordat: - uit het beleid – nader gespecificeerd in het privacybeleid - blijkt dat een zorgvuldige omgang met persoonsgegevens een kernwaarde van de Rechtspraak is; en - implementatie en concretisering van de BIO door IVO Rechtspraak. IVO Rechtspraak verwacht het laatste punt eind Q2 begin Q3 2022 te hebben afgerond.

2. Register van verwerkingsactiviteiten	
Norm	De organisatie registreert verwerkingsactiviteiten.
Referentie	Artikel 30 AVG Artikel 26c Wjsg
Beoordeling	
Kwaliteitsniveau: 3	De privacywet- en regelgeving stelt als eis dat persoonsgegevens rechtmatig worden verwerkt en dat dit aantoonbaar is. Het register van verwerkingsactiviteiten geeft in een oogopslag een integraal beeld van alle verwerkingen door een (of meerdere) verwerkingsverantwoordelijken. Per verwerking worden verschillende gegevens bijgehouden. Denk aan: het doel/de doelen van de verwerking, de verwerkingsgrondslag(en), de bewaartermijnen, de categorieën van persoonsgegevens, etc. Voorafgaand aan de inwerkingtreding van de AVG is door de projectleiding van het AVG-project van het Bureau Rvdr een landelijk verwerkingenregister opgesteld. Het landelijk register bevat de gemeenschappelijke gegevensverwerking door de Rechtspraak. Daarnaast heeft ieder gerecht onder eigen verantwoordelijkheid een lokaal register waarin de verwerkingen staan die naast de Rechtspraakbrede verwerkingen plaatsvinden. In dat kader is in samenwerking met IVO, gerechten en diensten het volgende gerealiseerd: - Landelijk register: ICT-applicaties (beheer privacy officer IVO); - Lokale registers: lokale IT en registraties (handmatig beheer gerechten en landelijke diensten zelf). Een samenvatting is te vinden via: register van verwerkingen. **Landelijk register** De Rvdr is als verwerkingsverantwoordelijke verantwoordelijk voor het vullen van het landelijke register. Het bijhouden en verder vullen omtrent de verwerkingen die landelijk plaatsvinden is door de Rvdr gemandateerd aan de privacy officer van IVO.

	Het landelijk register is afgerond en wordt op basis van nieuwe inzichten en nieuwe initiatieven constant bijgewerkt. **Lokale registers** De gerechten en landelijke diensten zijn verantwoordelijk voor het updaten van het lokale register. Er is in mei 2020 een inventarisatie gemaakt van de lokale registers door de beleidsmedewerker privacy van het bureau Rvdr om te onderzoeken in hoeverre de lokale registers voldoen aan de geldende privacywet- en regelgeving. In mei 2021 heeft een nieuwe inventarisatie plaatsgevonden. In beide gevallen is hiervoor het Key Control Dashboard gebruikt. Op basis van de inventarisatie van 2020 werd de conclusie getrokken dat de meeste gerechten en diensten een eerste stap hadden gezet met het register van verwerkingsactiviteiten. De registers gingen per verwerking echter niet in op alle vereisten uit de AVG. De gerechten en diensten zijn via de BVC'ers hierop geattendeerd. Uit de inventarisatie van 2021 blijkt dat in ieder geval drie gerechten aantoonbaar stappen hebben gezet. Daarnaast is geconstateerd dat verschillende gerechten de kwaliteit van het register borgen met een continue verbetercyclus. In het tweede kwartaal 2022 wordt een nieuwe inventarisatie uitgevoerd. Inmiddels hebben verschillende gerechten ervoor gekozen om gezamenlijk capaciteit beschikbaar te maken voor het bijwerken van het register van verwerkingsactiviteiten. **SmartPIA** In het kader van de registers van verwerkingsactiviteiten is de implementatie van SmartPIA relevant. Deze tool beoogt de administratie ten aanzien van het register van verwerkingsactiviteiten aanzienlijk te verminderen door, gebaseerd op de inhoud van de uitgevoerde en goedgekeurde PIA's automatisch het register te vullen. Periodieke herijking van een PIA zorgt dan ook voor aanpassing voor het register. Signalering hiervan vindt plaats via het systeem. Het register hoeft dan niet meer in een apart document te worden bijgehouden, maar wordt automatisch gegenereerd. Implementatie van SmartPIA heeft ervoor gezorgd dat is ingezien dat het landelijk register veel dubbele informatie bevat. Met SmartPIA wordt beoogd een gestroomlijnd register te verkrijgen waarmee ook inzicht wordt verkregen in de lokale verwerkingen. Over deze tool wordt in hoofdstuk 7 meer informatie gegeven.
Ambitieniveau: 5	De Rechtspraak kan met behulp van SmartPIA het hoogste kwaliteitsniveau halen. Op dit moment is duidelijk dat Rechtspraakbreed een basis is gelegd door middel van het opstellen van de registers van verwerkingsactiviteiten. In veel gevallen worden de registers periodiek geactualiseerd. Met de huidige middelen is er op centraal niveau nog beperkt inzicht in de registers, maar dit past binnen de verantwoordelijkheidsverdeling binnen de Rechtspraak. Met SmartPIA is er een centrale database waarin de lokale en landelijke verwerkingen staan. Het systeem zorgt eveneens voor een werkproces om de actualiteit van de registers te waarborgen. Tijdens het LOBRO van 3 maart 2022 maken de BVC'ers voor het eerst kennis met SmartPIA door middel van een presentatie.

	Om tot het hoogste kwaliteitsniveau te komen, moeten de volgende activiteiten worden uitgevoerd: - Implementatie van SmartPIA[4] (Samenwerking Bureau Raad en IVO, Q1 en Q2 2022)

3. Aantonen toestemming	
Norm	Het verlenen van toestemming wordt geregistreerd en kan worden aangetoond. Bij de grondslag toestemming wordt er rekening mee gehouden dat betrokkenen hun toestemming op ieder moment kunnen intrekken.
Referentie	Artikel 7, eerste lid AVG
Beoordeling	
Kwaliteitsniveau: 2	**De rol van toestemming voor de Rechtspraak** Toestemming in de zin van de AVG heeft voor de Rechtspraak, vergeleken met andere organisaties, een beperkte rol. De verwerkingen van de Rechtspraak worden – als overheidsorganisatie - grotendeels gebaseerd op de grondslagen: - wettelijke verplichting (art. 6, lid 1, sub c AVG); en - de taak van algemeen belang (art. 6, lid 1 sub e AVG). Bij innovatieve projecten, onderzoeken of in de bedrijfsvoering heeft toestemming als grondslag een iets grotere rol. **Documentatie van toestemming** Dit onderdeel is tweeledig. Ten eerste moet toestemming als grondslag in het register van verwerkingsactiviteiten bij een verwerking worden opgenomen. Over het register van verwerkingsactiviteiten is hierover het een en ander opgenomen (zie hiervoor KPI 2 ‘register van verwerkingsactiviteiten’). Ten tweede is het van belang dat de Rechtspraak de grondslag toestemming adequaat toepast. Hiervoor is ieder gerecht zelf verantwoordelijk. Dat betekent dat de gerechten en landelijke diensten ervoor moeten zorgen dat de gegeven toestemming kan worden aangetoond, dat betrokkenen de gegeven toestemming op ieder moment kunnen intrekken en dat ze voorafgaand aan het verlenen van toestemming alle informatie hebben ontvangen. Om na te gaan of de gerechten en diensten hier voldoende zicht op hebben is in de KCD-uitvraag van maart 2021 nagegaan of het inzicht aanwezig is en hoe de gerechten en diensten hiermee omgaan. De meeste gerechten en diensten hebben dit overzicht en geven aan te voldoen aan de vereisten van toestemming. Toestemming wordt slechts in een aantal verwerkingen gebruikt. Meest voorkomend zijn het faciliteren van opleidingen, deelname aan onderzoeken, bepaalde lijsten (bijv. verjaardagen) en HR-processen (bijv. bewaren van het CV).
Ambitieniveau: 3	Voor de Rechtspraak is het van belang dat voor ieder gerecht en voor iedere landelijke dienst te allen tijde duidelijk is bij welke verwerkingen de grondslag toestemming wordt gebruikt en dat het proces hieromtrent vastgelegd en geborgd is. De gerechten en diensten moeten blijven zorgen voor inzicht en een correcte toepassing van de grondslag toestemming. SmartPIA zal hier bij helpen.

[4] Zie hoofdstuk 7 over de implementatie van SmartPIA.

	Om de gerechten en diensten bij toekomstig gebruik van toestemming te helpen, is een kort overzicht gemaakt van de kaders die relevant zijn voor de grondslag toestemming. Deze is gedeeld met de BVC'ers na de KCD-uitvraag. Op dit moment zijn er geen aanvullende acties noodzakelijk met betrekking tot het ambitieniveau. Volgens de KPI's van JenV zijn nog twee stappen mogelijk, maar deze liggen vooralsnog niet in de rede. Het gaat dan om: - inrichten van lokale werkprocessen om de registratie van toestemming te controleren en te actualiseren. Iedere verwerking waarin toestemming wordt gebruikt is anders waardoor uniformering van het werkproces lastig wordt. Landelijke uniformering is beoogd met de hiervoor genoemde verstrekte kaders. - (elektronische) werkvormen om het verlenen en intrekken van toestemming te registreren. De verwachte voordelen van deze stappen ten opzichte van de kosten zijn beperkt, omdat toestemming beperkt als grondslag wordt gebruikt.

4. Registratie van datalekken	
Norm	De organisatie reageert aantoonbaar adequaat op datalekken en houdt een datalekregister bij.
Referentie	Artikel 33, vijfde lid AVG Artikel 26g jo. 51h Wjsg
Beoordeling	
Kwaliteitsniveau: 4	Sinds de zomer van 2016 is er een procedure voor het melden van datalekken. In oktober 2019 is deze procedure vernieuwd in het handboek datalekken. Daarnaast zijn enkele kleine wijzigingen aangebracht naar aanleiding van interne en externe signalen. De beveiligings- en privacycoördinatoren bij gerechten en diensten zijn verantwoordelijk voor de uitvoering van de procedure. Het registreren gebeurt met behulp van het softwarepakket Classbase. Op initiatief van het LOBRO is er door IVO een sharepointpagina ontwikkeld waarmee de registratie van datalekmeldingen geüniformeerd is. Dit systeem heeft als voordeel dat eventuele meldingen naar de toezichthouder direct gegenereerd kunnen worden. Met de Hoge Raad zijn afspraken gemaakt dat het formulier uit dit systeem door hen wordt geaccepteerd. De FG en de BVA zorgen, met hulp van de Medewerker BVA, voor overzichten ten behoeve van de viermaandsrapportage en het jaarverslag. Deze rapportages worden gedeeld met het LOBRO en het SBO, zodat zij kunnen kennisnemen van de resultaten en de daarop gebaseerde adviezen. Veel van de geconstateerde datalekken hangen samen met het verkeerd versturen van documenten (adresseringsfouten) of onvoldoende anonimisering van de uitspraken (anonimiseringsfouten). Om het aantal anonimiseringsfouten te verminderen, het anonimiseerproces te versnellen en vanwege de ambitie van de Raad van State, de Hoge Raad en de Rechtspraak om meer uitspraken te publiceren werkt IVO aan een anonimiseertool. Een tool is hiervoor reeds aangekocht. Momenteel wordt gewerkt aan de afronding van de installatie. In Q1 2022 start een pilot met een viertal gerechten, waarin de anonimiseertool functioneel en technisch getoetst zal worden. Op 2 december 2021 heeft de plv. FG de PIA die de pilot beschrijft van een positief advies voorzien.

	In januari 2022 is na onderzoek duidelijk geworden dat tussen 10 februari 2020 tot en met 25 januari 2022 3153 adresseringsfouten hebben plaatsgevonden door de digitale postkamer. Deze aantallen waren nog niet eerder bekend. De beveiligingscoördinatoren waren hiervan ook niet op de hoogte. Op hun verzoek is daarom een uitsplitsing verstuurd waarin per gerecht en per zaakstroom het aantal adresseringsfouten staan. Zij hebben tegelijkertijd ook een verdere specificatie ontvangen van de individuele gevallen, zodat nader onderzoek mogelijk is.
Ambitieniveau: 5	Het hoogste kwaliteitsniveau is haalbaar voor de Rechtspraak. Om hiertoe te komen is vereist dat de organisatie over een optimale, voor de organisatie passende werkvormen voor de afhandeling en registratie van datalekken beschikt. Het LOBRO constateert dat er nog een verschil is in de gevallen waarin melding van een datalek wordt gedaan. Het ene gerecht meldt alles en sommige gerechten uitsluitend ‘ernstige’ datalekken. Daarnaast meldt het ene gerecht in Classbase en andere gerechten via de sharepointpagina. In 2021 is geprobeerd meer uniformiteit te krijgen, maar dat kan met het oog op de eigen verantwoordelijkheid van ieder gerecht niet worden afgedwongen. Het punt wordt in het (DB) LOBRO aan de orde gesteld en opgepakt door de portefeuillehouder privacy van het DB LOBRO. Dit moet resulteren in een tweetal punten: 1. Rechtspraakbreed gebruik maken van één registratiesysteem. 2. Rechtspraakbrede afspraken maken over het melden van datalekken. Tot slot moeten op korte termijn aanpassingen worden verricht in de digitale postkamer om het aantal adresseringsfouten te verminderen. Op 4 februari 2022 is een extra controle op zaaksoort geïmplementeerd. Hierdoor krijgt men voortaan een waarschuwing te zien als de zaaksoort niet dezelfde is als bij de indiening. Daarnaast wordt met het Digitaal Zaaksdossier gewerkt aan een structurele oplossing. Naar verwachting wordt die in 2023 opgeleverd. Het privacyteam van IVO ziet op de oplevering van DZD toe. Acties: • Afspraken uniforme melding datalekken (LOBRO; eind 4e kwartaal 2022) • Experiment en landelijke uitrol anonimiseertool (projectleider anonimisering bij IVO; uitrol van de anonimiseertool begint – onder voorwaarden – in 2022). • Aanpassen digitale postkamer om datalekken te verminderen. (Projectteams DT en DZD van IVO; beoogde update begin 2023).

5. Verwerking met betrekking tot derde partijen

Dit hoofdstuk geeft inzicht in de mate waarin door de Rechtspraak afspraken zijn gemaakt met andere partijen indien de persoonsgegevens de organisatie overschrijden. Extra aandacht gaat uit naar afspraken met partijen waarbij persoonsgegevens de grenzen van de Europese Economische Ruimte overschrijden.

Bij dit onderdeel is het van belang onderscheid te maken tussen:

- Een verwerkingsverantwoordelijke: stelt het doel (waarom?) en middelen (hoe?) vast van een verwerking.
- Een (sub)verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Uit het voorgaande kunnen vier soorten relaties worden onderscheiden: de relatie tussen

- verwerkingsverantwoordelijke en verwerker: de verwerkingsverantwoordelijke besteedt de verwerkingen uit aan een verwerker. In dit geval moet een verwerkersovereenkomst afgesloten.
- Twee of meer verwerkingsverantwoordelijken: een verwerkingsverantwoordelijke deelt gegevens met een partij die zelf doel en/of de middelen bepaalt voor de verwerking. Een voorbeeld hiervan is het uitvoeren van een onderzoek. In dit geval kunnen privacyafspraken of gegevensleveringsovereenkomsten worden afgesloten.
- Verwerkingsverantwoordelijken gezamenlijk: twee of meer partijen stellen gezamenlijk het doel en de middelen voor de verwerking vast. In dit geval moeten privacyafspraken worden afgesloten.
- twee organisaties die onder de Staat der Nederlanden vallen: in dat geval worden privacyafspraken afgesloten tussen de beide organisaties, omdat in juridisch sprake is van één organisatie.

Uit de PIA blijkt van welke relatie sprake is en dus welk soort overeenkomst is vereist.

5. Verwerkingen door verwerkers	
Norm	De organisatie legt onderlinge afspraken met verwerkers vast.
Referentie	Artikel 28, derde lid AVG Artikel 7, 7d en 26c lid 2 Wjsg.
Beoordeling	
Kwaliteitsniveau: 4	Bij dit onderwerp wordt een onderscheid gemaakt tussen: • de landelijke contracten afgesloten door IVO; • de contracten afgesloten door de individuele gerechten en andere landelijke diensten via het LDCR. **IVO** Het gaat hier om het afsluiten van privacyafspraken of verwerkersovereenkomsten voor systemen die landelijk worden gebruikt. De resterende verwerkersovereenkomsten worden in orde gemaakt. Er dienen nog voor enkele diensten verwerkersovereenkomsten te worden getekend. Daarbij dient te worden opgemerkt dat voor sommige diensten gezamenlijk met andere organisaties een verwerkersovereenkomst moet worden opgesteld. Denk hierbij aan grote ICT-leveranciers als Microsoft, Adobe en Citrix. Er zijn reminders verstuurd, maar dit heeft nog niet tot wezenlijke vooruitgang gezorgd. **Gerechten en andere landelijke diensten** Na de beveiligingsbenchmark van 2019 is in de KCD-uitvraag van maart 2021 opnieuw uitgevraagd of gerechten verwerkersovereenkomsten hebben afgesloten waar nodig. Bij de meeste gerechten en diensten zijn de overeenkomsten afgesloten. Bij enkele gerechten en andere landelijke diensten zijn verbeterpunten geconstateerd. **Bewustzijn** Ten aanzien van dit punt wordt geconstateerd dat steeds meer bewustwording ontstaat ten aanzien van de verwerkersovereenkomst. Dit past bij het beeld dat het privacybewustzijn steeds verder groeit als gevolg van interne en externe

	berichtgeving. Daarnaast vragen leveranciers vanuit hun eigen verantwoordelijkheid steeds vaker om een verwerkersovereenkomst af te sluiten. Tot slot dragen de werkprocessen bij de inkoopafdelingen bij aan een toename in verwerkersovereenkomsten. **Wegvallen privacy shield** De gevolgen van het privacy shield bij de verwerking van persoonsgegevens van de Rechtspraak in de VS is ook relevant voor verwerkersovereenkomst. Het model verwerkersovereenkomst is naar aanleiding van de uitspraak van het Hof van Justitie van de EU aangepast. Bestaande overeenkomsten moeten ook worden aangepast. Meer hierover staat onder punt 7.
Ambitieniveau: 5	De Rechtspraak heeft nog niet voor alle externe datadelingen privacy-afspraken of een verwerkersovereenkomst opgesteld. Wel heeft de Rechtspraak in beeld waarvoor nog overeenkomsten afgesloten moeten worden en op welke punten nog actie is vereist. De dienstenmanagers zijn op de hoogte. SP&K monitort en spreekt aan waar nodig. Verder is het van belang dat intern afspraken worden gemaakt om te borgen dat verwerkersovereenkomsten en privacyafspraken periodiek worden geëvalueerd en worden geactualiseerd. Hiermee wordt geborgd dat afspraken voor de duur van de overeenkomst blijven voldoen aan de wederzijdse verplichtingen van de privacywet- en regelgeving. Acties: • Bij de KCD-uitvraag voor 2022 zal opnieuw worden gevraagd in hoeverre alle gerechten verwerkersovereenkomst/privacyafspraken hebben afgesloten met verwerkers of andere verwerkingsverantwoordelijken(Adviseur privacy & informatiebeveiliging, 2e kwartaal 2022). • Afsluiten nog ontbrekende verwerkersovereenkomsten/ privacyafspraken door IVO. Dienstenmanagers zijn op de hoogte; SP&K monitort. • Borgen van periodieke evaluatie en actualisatie van verwerkersovereenkomsten/privacyafspraken (Privacy officer/ Adviseur privacy en informatiebeveiliging, Q4 2022)

6. Gezamenlijke verantwoordelijkheid	
Norm	Indien de organisatie samen met een andere partij gezamenlijk het doel en middel van de verwerking bepaalt worden onderlinge afspraken over hoe de verantwoordelijkheden zijn verdeeld geregistreerd.
Referentie	Artikel 26 AVG Artikel 26c Wjsg
Beoordeling	
Kwaliteitsniveau: 3	Gezamenlijke verwerkingsverantwoordelijkheid houdt in dat de Rechtspraak samen met een andere organisatie of partij de doelen van en de middelen voor een verwerking vaststellen. Dit is het geval in de relatie tussen de Raad voor de rechtspraak en de gerechten, omdat ieder gerecht en de Raad voor de rechtspraak ieder voor zich verwerkingsverantwoordelijk zijn. In het kader van de onderlinge verhoudingen zijn afspraken gemaakt in diverse documenten. Zo valt te denken aan de governance documenten voor privacy en het informatieprotocol.

	Andere gevallen waarin sprake is van gezamenlijke verwerkingsverantwoordelijkheid komen niet vaak voor. Veelal worden de doelen van en de middelen van verwerking bij een opdracht door de partijen zelf bepaald en niet gezamenlijk. Een voorbeeld hiervan is een onderzoeksopdracht waarbij de Rechtspraak de doelen bepaalt en de onderzoekers de middelen.
Ambitieniveau: 3	Op dit moment zijn er geen signalen die nopen tot acties om het kwaliteitsniveau te verhogen.

7. Doorgifte van persoonsgegevens buiten de EER	
Norm	Doorgifte van persoonsgegevens naar landen en organisaties buiten de EER vindt gecontroleerd plaats en wordt geregistreerd.
Referentie	Artikel 44 en 49 AVG; Artikel 16a, 26d, tweede lid Wjsg
Beoordeling	
Kwaliteitsniveau: 3	Van doorgifte van persoonsgegevens aan een derde land is sprake wanneer persoonsgegevens buiten de Europese Economische Ruimte worden gebracht. Denk hierbij aan het versturen of opslaan van persoonsgegevens in de Verenigde Staten. In dit kader zijn vier punten relevant. Ten eerste zijn er binnen de Rechtspraak 15 applicaties die persoonsgegevens buiten de Europese Economische Ruimte (EER) versturen. Door de vernietiging van het adequaatheidsbesluit (Privacy Shield) door het Hof van Justitie van de EU is door de dienstenmanagers samen met SP&K IVO in kaart gebracht wat de impact daarvan is voor de Rechtspraak. Op basis van de resultaten moet worden bepaald of de Rechtspraak na het wegvallen van het US-EU Privacy Shield in control is. Hiervoor zijn o.a. de volgende vragen van belang: 1) Wat hebben we als Rechtspraak staan in Amerikaanse cloud of staat in EER maar heeft risico van doorgifte naar VS? 2) Wat is juridisch/technisch mogelijk/noodzakelijk om te regelen? 3) Welke maatregelen neemt (IVO) Rechtspraak? De uitkomsten hiervan worden aan de directie van IVO voorgelegd. In het kader van de verwerking van persoonsgegevens buiten de EER heeft de AP als onderdeel van een breder onderzoek in Europees verband op 15 februari 2022 aangekondigd onderzoek te gaan doen op het gebruik van cloudvoorzieningen bij overheidsinstanties. In de aankondiging is aangegeven dat overheidsinstanties een vragenlijst krijgen. Gezien de beperkte bevoegdheid van de AP ten aanzien van de gerechten in hun gerechtelijke taak, is nog niet duidelijk wat de impact hiervan is. Ten tweede is noemenswaardig de relatie met het Gemeenschappelijk Hof van Justitie van de Nederlandse Antillen. Op dit moment vinden nog geen gegevensuitwisselingen plaats tussen de Rechtspraak en het Gemeenschappelijk Hof. Het is niet uitgesloten dat dit in de toekomst zal veranderen. Ten derde is het cloudbeleid op 12 juli 2021 vastgesteld door het PRO, nadat de S&I- board en de Raad op 2 februari 2021 resp. 17 februari 2021 akkoord zijn gegaan. Het cloudbeleid van de Rechtspraak biedt kaders voor het gebruik van clouddiensten. Het cloudbeleid wordt verder uitgewerkt in andere documenten, zoals een control framework en een cloudstrategie. Het team SP&K van IVO Rechtspraak werkt aan handreikingen die hierop aansluiten. Het cloudbeleid zal periodiek geactualiseerd worden. Om de kaders en de

	kennis te structureren en te borgen, is er een cloudregiegroep en een cloud competence centre opgericht. Tot slot is als gevolg van de Brexit het Verenigd Koninkrijk een derde land. In het verdrag tussen de EU en het VK is een regeling opgenomen om ervoor te zorgen dat het uitwisselen van persoonsgegevens mogelijk blijft. Op 28 juni 2021 zijn door de Europese Commissie twee adequaatheidsbeslissingen genomen voor uitwisseling van persoonsgegevens met het VK. Het gaat om een adequaatheidsbesluit om persoonsgegevens in het kader van de AVG en de Richtlijn.[5]
Ambitieniveau: 5	Om tot niveau 5 te komen is het van belang dat in lijn met punt 3 van KPI 5 (‘verwerkingen door verwerkers) ook hier een periodieke evaluatie en actualisatie van de overeenkomsten plaatsvindt. In het verlengde daarvan worden naar aanleiding van de vernietiging van het US-EU Privacyshield door het Europees Hof van Justitie nadere verwerkersovereenkomsten door IVO opgesteld voor de bestaande diensten in de Amerikaanse cloud. Nieuwe diensten die de cloud in willen moeten daarvoor eerst langs de cloudregiegroep om goedkeuring te krijgen. Voor de nieuwe Amerikaanse clouddiensten geldt dat in de verwerkersovereenkomst rekening moet worden gehouden met de opheffing van het US-EU. Privacy Shield. De standaard verwerkersovereenkomst is daarom aangepast.

[5] Adequacy decisions | European Commission (europa.eu), geraadpleegd 5 juli 2021

6. Privacy by Design en Privacy by Default

Met privacy by design wordt inzicht gegeven in de mate waarin rekening wordt gehouden met het kwaliteitsaspect privacy als aandachtspunt bij het ontwikkelen van nieuwe (werk)processen, informatiesystemen en/of beleid of wetgeving. Met privacy by default wordt beoogd (werk)processen, informatiesystemen en/of beleid te leveren die standaard uitgaan van de minst inbreukmakende gegevensverwerking.

De focus van de KPI's liggen bij het beschermen van de persoonsgegevens van de betrokkenen van wie persoonsgegevens door de Rechtspraak worden verwerkt.

8. Privacy by Design & Privacy by Default	
Norm	De organisatie houdt al in de ontwikkelfase van een verwerking aantoonbaar rekening met een zorgvuldige omgang met persoonsgegevens (privacy by design). Bij het presenteren van een keuze worden aan betrokkene privacyvriendelijke instellingen aangeboden (privacy by default).
Referentie	Artikel 24 en 25, eerste lid en tweede lid AVG Artikel 7 en 7a Wjsg
Beoordeling	
Kwaliteitsniveau: 2	Ten aanzien van privacy in de ontwerpfase is een onderscheid te maken tussen: - ontwikkelingen bij IVO; - ontwikkelingen bij gerechten en andere diensten. **IVO** De meeste ICT-ontwikkelingen vinden plaats bij IVO Rechtspraak. IVO werkt aan de implementatie van privacy by design en privacy by default in het ontwikkelproces. Bij steeds meer ontwikkelingen wordt privacy by design gebruikt, maar een structurele aanpakt waarbij privacy daadwerkelijk vanaf het begin betrokken is, is nog in ontwikkeling. Hiervoor wordt samengewerkt met de ontwikkelteams. Daarnaast werkt de CISO/Teamleider SP&K aan een verbeterplan en een checklist Security & privacy. Uiteindelijk zal SmartPIA ook bijdrage aan privacy by design. Het wel of niet aanpassen van de ICT-systemen om deze in lijn met de privacywet- en regelgeving te brengen wordt besproken onder punt 10 'Waarborgen van een passend beveiligingsniveau' besproken. **Gerechten en andere landelijke diensten** De concepten privacy by design en privacy by default zijn bij de gerechten en andere landelijke diensten groeiende. Voor gerechten en diensten is duidelijk dat privacywet- en regelgeving van belang is. Steeds meer gerechten stellen hiervoor capaciteit beschikbaar. Daarnaast wordt ook bij het ministerie van Justitie en Veiligheid in het kader van de prijsonderhandelingen 2023-2026 budget gevraagd om o.a. privacy te borgen. Ondanks dat privacywet- en regelgeving nog niet optimaal is geborgd, vallen vooralsnog geen (grote) steken in de zin van datalekken. Collega's binnen de Rechtspraak weten de privacy experts steeds vaker te vinden voor advies. Daarnaast zorgen de afgesproken werkprocessen voor voldoende achtervang.
Ambitieniveau: 3	De gerechten en de landelijke diensten moeten nog groeien in het borgen van privacy voorafgaand aan de start van de verwerking. De eisen van de AVG komen nu pas om de hoek kijken als een gegevensverwerking al gestart is. Verder ontbreekt een cyclische werkwijze waarbij:

	1) privacyrisico's vanaf dag één in kaart worden gebracht, 2) de maatregelen ter mitigatie van de risico's tijdens de ontwikkeling worden geïmplementeerd, 3) de maatregelen in het register van verwerkingsactiviteiten worden opgenomen en 4) periodiek op de effectiviteit van de maatregelen gecontroleerd wordt. Dit laatste kan leiden tot eventuele aanpassingen. Hiervoor moeten de volgende actie worden ontplooid: - Verder implementeren van privacy by design bij IVO Rechtspraak en gerechten door o.a. het uitvoeren van PIA's en het bijwerken van het register van verwerkingsactiviteiten voorafgaand aan de start van een verwerking. In de toekomst kan het ambitieniveau worden verhoogd naar 4 of 5. Voor die stappen is vereist dat de naleving van de aantoonbare zorgvuldige omgang en het aantoonbare privacyvriendelijke aanbod aan betrokkene wordt gemonitord (4) en dat hiervoor optimale en passende werkvormen zijn (5). Vooralsnog blijven deze stappen buiten beschouwing om acties goed te kunnen focussen en de onderwerpen gestructureerd te laten groeien.

9. Privacy Impact Assessments (PIA)	
Norm	Bij verwerkingsactiviteiten voert de organisatie indien van toepassing PIA's uit.
Referentie	Artikel 35 AVG Artikel 7b Wjsg
Beoordeling	
Kwaliteitsniveau: 2	De privacywet- en regelgeving stelt dat alleen een PIA moet worden uitgevoerd wanneer er een hoog risico is voor de privacy van betrokkenen. De Rechtspraak hanteert echter een omgekeerd beleidsuitgangspunt: een PIA moet altijd voorafgaand aan de start van een verwerking worden uitgevoerd, tenzij de risico's met het oog op de inspanning laag zijn. Hiervoor zijn twee redenen: - de aard van de Rechtspraak als overheidsorganisatie en staatsmacht brengt mee dat in beginsel sprake is van een hoog risico voor betrokkenen; - het uitvoeren van een PIA draagt bij aan de documentatieplicht genoemd onder hoofdstuk 4 'Privacyadministratie'. De status van dit aandachtspunt wordt uitgesplitst naar de situatie bij: 1) IVO Rechtspraak; 2) de gerechten en overige diensten. Hierbij kan opgemerkt worden dat PIA's nu nog plaatsvinden conform het Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) of een PIA Light. In eind Q1, begin Q2 2022 begint de overstap naar SmartPIA stapsgewijs. **IVO Rechtspraak** De Rechtspraak maakt gebruik van een mix van oudere en nieuwe systemen. Deze systemen worden veelal door IVO Rechtspraak beheerd. Van de oude systemen zijn voor de invoering van de AVG en de Wjsg geen PIA uitgevoerd. De PIA's die wel zijn uitgevoerd, zijn veelal niet meer actueel. Deze PIA's worden met terugwerkende kracht alsnog opgesteld en bijgewerkt. Voor nagenoeg alle primaire processystemen is in 2019 en 2020 een PIA opgesteld.

	Daarnaast zijn er ook PIA's uitgevoerd op de secundaire processystemen. Het is echter onduidelijk of op alle systemen reeds een PIA is uitgevoerd. Om nieuwe omissies te voorkomen wordt sinds 2016 elk nieuw (te ontwikkelen) systeem onderworpen aan een PIA. Bij aanpassingen in het systeem wordt de bestaande PIA herijkt. Buiten eventuele aanpassingen moet de PIA ieder jaar worden bijgewerkt. Om het proces voor het uitvoeren van PIA's te borgen is door IVO een procesbeschrijving opgesteld. De procesbeschrijving gaat in op het uitvoeren van PIA's voor nieuwe projecten, bestaande diensten en de periodieke herijking van PIA's. Dit is een samenwerking waar ook vertegenwoordigers vanuit de business bij aansluiten. **Gerechten en overige diensten** Ieder gerecht heeft een register van lokale verwerkingsactiviteiten (zie KPI 2). Aan iedere verwerking in het register moet een PIA ten grondslag liggen waaruit de informatie voor het register blijkt. Denk aan het doel van de verwerking, de bewaartermijn en de ondersteunende systemen. Ter controle van dit proces is in april 2020 via het Key Control Dashboard (KCD) uitgevraagd in hoeverre de nodige lokale PIA's zijn uitgevoerd. Uit de uitvraag is gebleken dat PIA's nog onvoldoende plaatsvinden vanwege een gebrek aan kennis. Daarom is eind september 2020 een cursus gegeven aan de privacycoördinatoren om de benodigde kennis bij te brengen. Begin 2021 heeft een vervolgcursus plaatsvonden. Hierin is ook het cyclische karakter van de PIA besproken. Inmiddels hebben verschillende gerechten ervoor gekozen om gezamenlijk capaciteit beschikbaar te maken voor het bijwerken van het register van verwerkingsactiviteiten en het opstellen van PIA's. Daarnaast zijn door verschillende gerechten de eerste PIA's uitgevoerd. Ondanks dat het aantal PIA's bij de gerechten nog achterblijft, wordt het overgrote deel van de verwerkingen afdekt met PIA's die door IVO zijn en worden uitgevoerd. Daarnaast signaleert het LDCR als een PIA ontbreekt bij de aankoop van een nieuwe dienst of systeem. Het LDCR geeft dit bij het betreffende gerecht aan.
Ambitieniveau: 5	Door het uitvoeren van de volgende twee verbeteracties is de Rechtspraak in staat tot het hoogste ambitieniveau te behalen, omdat er dan een optimale voor de organisatie passende werkvorm is voor het houden van PIA's en de registratie daarvan. 1) <u>Bestuurlijke vaststelling van PIA's en de acceptatie/mitigatie van risico's</u> Als de PIA is uitgevoerd, moet de PIA bestuurlijk worden vastgelegd. Uit de Privacy Governance Rechtspraak blijkt dat in geval van een gerechtsoverstijgende PIA de Raad en de gerechtsbesturen als gezamenlijk verwerkingsverantwoordelijken de PIA moeten goedkeuren. Het voorleggen van een PIA aan (veelal) het PRO is echter niet voor iedere PIA noodzakelijk. Aan vereenvoudigingsstructuur wordt gewerkt. Het reeds vastgestelde Addendum Privacy Governance wordt op basis van het voorstel vanuit het Bureau BVA aangevuld met een mandateringsstructuur om het vaststellen van PIA's en de bijbehorende risico's te vereenvoudigen. 2) <u>Implementatie SmartPIA:</u>

	In 2022 wil de Rechtspraak gebruik gaan maken van de tool SmartPIA. Deze tool zal: - het PIA-proces versnellen door het automatiseren; - de kwaliteit verbeteren doordat de tool de gebruiker kennis aanreikt; - signaleren als een PIA na een bepaalde periode moet worden herijkt; - automatisch het register van verwerkingsactiviteiten bijwerken. De status van de tool wordt onder hoofdstuk 10 beschreven.

10. Waarborgen van een passend beveiligingsniveau[6]	
Norm	Bij verwerkingsactiviteiten voert zorgt de organisatie voor een passend beveiligingsniveau.
Referentie	Artikel 5, eerste lid, sub f , 24 en 32 AVG Artikel 7, tweede lid Wjsg
Beoordeling	
Kwaliteitsniveau	De privacywet- en regelgeving schrijft voor dat persoonsgegevens op een passende manier moeten worden beveiligd. Dit betekent dat rekening moet worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. In deze KPI wordt uitgebreid stilgestaan bij verschillende onderdelen die binnen deze norm passen. Ter bespreking hiervan wordt een onderscheid gemaakt in: compliancy landelijke ICT-systemen, bewaartermijnen, het wegwerken van auditbevindingen, logging en autorisatiebeheer. **Compliancy landelijke ICT-systemen** Als informatievoorzieningsorganisatie moet IVO ervoor zorgen dat de ICT-systemen in lijn zijn met de privacywet- en regelgeving. Daarom is door IVO in 2018 een project gestart dat – na verschillende aanpassingen van de scope – privacy impact analyses uitvoert om te bepalen welke aanpassingen gerealiseerd moeten worden om de ICT-systemen in lijn te brengen met de geldende privacywet- en regelgeving. Uiteindelijk is het aan de dienstenmanagers en portefeuillehouders om de aanpassingen in de systemen door te voeren. Dit project heeft na het uitvoeren van de systeemanalyses décharge gekregen van de directie van IVO. Al lange tijd is niet duidelijk wanneer de systemen aangepast zullen zijn aan de geldende wet- en regelgeving.[7] De CIO/Algemeen directeur van IVO heeft hierover verschillende keren gesproken met de Raad. Sindsdien zijn door IVO verschillende stappen ondernomen. Tijdens de werkgroep privacy van 22 december 2021 is door de portefeuillehouder bedrijfsvoering een toelichting gegeven. De leden van de

[6] Aan deze KPI worden geen kwaliteitsniveau en ambitieniveau gekoppeld, omdat deze KPI niet afkomstig is uit privacymanagement KPI's van JenV, maar de Rechtspraak zelf heeft toegevoegd om te zorgen voor een volledige rapportage.
[7] Op basis van een risicoafweging kan er ook voor worden gekozen om systemen niet aan te passen, maar het risico te accepteren.

	Werkgroep hebben de mogelijkheid gehad hierop te reageren. Vanuit het Bureau Raad is door de directeur, FG en de plv. FG reactie gegeven. Deze opmerkingen zijn verwerkt in de AVG-notitie met bijlagen en geagendeerd voor de Raad op woensdag 23 maart 2022. Op 1 februari was nog niet duidelijk wanneer de planning voor de compliancy van de landelijke ICT-systemen wordt opgeleverd. Dat betekent dat de Rechtspraak t.a.v. dit punt niet volledig in control is. Bij non-compliancy loopt de Rechtspraak niet alleen het risico op een boete, maar ook om niet te voldoen aan de loggingsverplichting uit Richtlijn (zie hierna). **Bewaartermijnen** Voor de Rechtspraak zijn de bewaartermijnen vastgelegd in zogenoemde 'Basis Selectie Documenten' (BSD). Deze zijn: - Het BSD Rechtelijke macht (geactualiseerd januari 2021): https://www.nationaalarchief.nl/archiveren/kennisbank/primair-proces-van-de-rechtspraak-selectielijst-voor-de-waardering-van-alle - Het BSD Bedrijfsvoering Rechtspraak (inclusief P-dossier): https://zoek.officielebekendmakingen.nl/stcrt-2018-23197.html Door het ministerie zijn nieuwe selectielijsten opgesteld en gepubliceerd. De Rechtspraak heeft vervolgens haar eigen lijsten aangepast. De systemen en processen moeten echter nog zodanig worden ingericht dat conform deze lijsten wordt gewerkt. Op basis van deze richtlijnen dienen de concrete bewaartermijnen per (onderdeel van een) systeem te worden opgetekend. In principe zijn de basisselectiedocumenten zowel voor papier als voor gegevens opgenomen in digitale systemen. Door de IVO-portefeuillehouder Generieke systemen/Bedrijfsvoering is, in afstemming met medewerkers van het Bureau Rvdr, een beleidslijn bewaartermijnen van digitaal opgeslagen persoonsgegevens in het kader van de behandeling van gerechtelijke stukken opgesteld. Dit document is op 14 februari 2022 door het SBO goedgekeurd. In aanvulling op deze beleidslijn is op verzoek van de adviseur privacy en informatiebeveiliging een onderzoek gestart naar een wijze waarop omgegaan kan worden met bewaartermijnen in niet-zaaksgebonden processen. Het rapport van dit onderzoek wordt in het eerste kwartaal van 2022 verwacht. Op basis van het rapport wordt een beleidslijn bewaartermijnen niet-zaaksgebonden processen opgesteld die als aanvulling geldt op de beleidslijn van de IVO-portefeuillehouder. Deze beleidslijn zal – na interne afstemming – ook aan het SBO worden voorgelegd. **Het wegwerken van auditbevindingen** In 2019 heeft de actie gelopen om de auditbevindingen t.a.v. informatie-beveiliging op te schonen. Dit heeft erin geresulteerd dat in 2019 in totaal 195 bevindingen zijn afgesloten. In 2020 zijn vervolgens 142 bevindingen weggewerkt waardoor er nog 353 bevindingen open staan. Dit aantal is in 2021 teruggebracht tot 245 (peildatum 22 juni 2021). De verdeling in prioriteit wordt in onderstaande tabel weergegeven.

Prioriteit	Totaal	Alleen 2020 en 2021 bevindingen
Hoog	47	0
Midden	138	53
Laag	60	43

Het is in eerste instantie een verantwoordelijkheid van de toegewezen dienst of instantie.

Logging
De Wjsg, AVG en UAVG vereisen logging van gebruikershandelingen door de systemen. Door het ministerie van Justitie en Veiligheid is op 1 januari 2019 een KB gepubliceerd waarmee uitstel is verleend van de loggingsverplichting die geldt voor systemen in het strafdomein.

De deadline om aan de loggingsverplichting in artikel 63, tweede lid Richtlijn te voldoen verloopt op 6 mei 2023. Er is een mogelijkheid om dispensatie van de Europese Commissie te krijgen tot mei 2026, maar daarvoor moet het ministerie een onderbouwd verzoek indienen. De Rechtspraak heeft daarom tot doel om op 31 december 2022 aan de loggingsverplichting te voldoen. Is dat niet mogelijk, dan zijn er nog 5 maanden om een dispensatieverzoek in te dienen.

De Rechtspraak is hier in grote mate afhankelijk van het OM, omdat de Rechtspraak verschillende strafsystemen van het OM gebruikt. Desalniettemin heeft de Europese wetgever de loggingsverplichting bij de verwerkingsverantwoordelijke gelegd. De Rechtspraak is verwerkingsverantwoordelijk voor de gerechtelijke strafgegevens. Hierdoor blijft de Rechtspraak verantwoordelijk om ten aanzien van de gerechtelijke strafgegevens aan artikel 63, tweede lid Richtlijn te voldoen. Het gebruik van OM systemen maakt dat niet anders.

Verder wordt door IVO Rechtspraak naar aanleiding van de BKBO-audit in 2020 gewerkt aan een loggingsdocument.

Autorisatiebeheer
Het autorisatiebeleid is volgens de huisaccountant niet op orde en de belangrijkste bevindingen waren[8]:

- het ontbreken van (uniforme) procedurebeschrijvingen omtrent het toekennen, wijzigen en tijdig ontnemen van rechten in de primaire processystemen;
- het ontbreken van inzicht in welke gebruikers over welke toegangsrechten beschikken in de primaire processystemen;
- het ontbreken van een periodieke controle op de juistheid van de toegekende rechten aan gebruikers in de primaire processystemen.

Om deze punten op te pakken loopt – na afronding van het project SIMS – nog een project: informatierotonde.

Dit project is samen met functioneel beheer van IVO gestart na de bevindingen van de accountant. Om inzicht te krijgen, maakt het project gebruik van de

[8] PricewaterhouseCoopers Accountants N.V., Raad voor de rechtspraak Controle 2020 Rapportage interimbevindingen (Management Letter), 7 dec 2020.

	informatierotonde, waarmee het mogelijk wordt om diverse gegevensbestanden van samenhang te voorzien en daaruit output te generen. Inmiddels is het project zover dat een groot aantal systemen (bijv. Civiel, Berber, Reis, Nias, Gps, Compas, GPS, Klaver, Mars, Leonardo, Ebilling, etc.) in de informatierotonde zijn gekoppeld en dat gerechten zijn voorzien van 'foutenlijsten' waarmee zij de systemen kunnen opschonen. Met de publieke aandacht voor de problemen rondom de autorisaties bij de Politie, het UWV en recent ook de GGD komt ook voor de Rechtspraak de vraag op of dit bij ons wel goed geregeld is. Met de informatierotonde wordt hard gewerkt om hierin inzicht te verkrijgen. Daarna moet worden bepaald wie welke rechten mag hebben en of dit conflicten oplevert. Daarnaast merken de gerechten nu welke meerwaarde de informatierotonde heeft en komen er meermaals verzoeken om nog meer bestanden te koppelen. Na de opzet van een hoedanighedenplatform (een vervolg op de informatierotonde) wordt het mogelijk om ook de beveiligingsniveaus van informatie vast te leggen (classificatie of rubricering).
Ambitieniveau	Ten aanzien van de acties wordt eenzelfde onderscheid gemaakt als hiervoor: compliancy landelijke ICT-systemen, bewaartermijnen, het wegwerken van auditbevindingen, logging en autorisatiebeheer. Compliancy landelijke ICT-systemen: • Opstellen van een planning op welk moment de ICT-systemen zijn aangepast, zodat ze voldoen aan de verplichten uit de geldende privacywet- en regelgeving. Dit kan ook betekenen dat systemen niet worden aangepast. • De portefeuillehouder in de Raad geeft aan dat er met betrekking tot het belang van privacy en informatiebeveiliging ook een structurele communicatie aanpak nodig is. Van belang is dat bij nieuwe projecten tijdig aandacht aan privacy en informatiebeveiliging wordt geschonken. Bewaartermijnen: • Opstellen beleidslijn werkwijze bewaartermijnen niet-zaaksgebonden gegevens naar aanleiding van het uitgevoerde onderzoek (Adviseur privacy en informatiebeveiliging, Q4 2022). Het wegwerken van auditbevindingen: • De trend van openstaande bevindingen gaat gestaag naar beneden, als deze zich voortzet zal in 2025 de achterstand in bevindingen zijn weggewerkt. Dit gaat lukken als de focus op het oplossen van de bevindingen blijft. Dit blijft het team SP&K monitoren door met de desbetreffende afdelingen in gesprek te blijven over het afronden van de openstaande bevindingen of maatregelen. Logging: • Het loggingsbeleid moet door de directie van IVO worden goedgekeurd. • Het IT-normenkader logging wordt op basis van het nieuwe loggingsbeleid aangepast. • Verder werkt IVO aan een centrale voorziening voor logging. Autorisatiebeheer: • De adviseur privacy & informatiebeveiliging volgt de voortgang van het project informatierotonde.

7. Transparantie

Transparantie geeft aan op welke wijze de verwerkingsverantwoordelijke namens diens organisatie invulling geeft aan het transparantiebeginstel, dat onderdeel uitmaakt van het hoofdstuk over Rechten van Betrokkenen van de AVG. Transparantie is een onderdeel van de informatieplicht die op de verwerkingsverantwoordelijke rust en gaat over gepaste openheid over de gehanteerde zorgvuldigheid bij het verwerken van persoonsgegevens.

11. Informeren van betrokkenen	
Norm	De organisatie informeert de betrokkene tijdig en op begrijpelijke wijze over de gegevensverwerking.
Referentie	Artikel 5, eerste lid, art. 13 en 14 AVG Artikel 17 t/m 26 Wjsg
Beoordeling	
Kwaliteitsniveau: 3	Bij dit aandachtspunt gaat het over de informatie die onder andere in de privacyverklaring is opgenomen. Op rechtspraak.nl/privacy worden de 5w- en h- vragen beantwoord onder de veelgestelde vragen. Verder gelden voor de bewaartermijnen van documenten in het primaire proces de basisselectiedocumenten. Deze zijn gepubliceerd op nationaalarchief.nl. Voor rechtszoekenden en professionals moet het eenvoudig zijn om informatie te vinden over de wijze waarop de Rechtspraak omgaat met persoonsgegevens. De Rechtspraak heeft op twee plekken een privacyverklaring gepubliceerd: - een algemene op rechtspraak.nl; en - een verklaring die aansluit bij de sollicitatieprocedure van de Rechtspraak. Indien betrokkenen meer informatie willen ontvangen over de wijze waarop de Rechtspraak omgaat met persoonsgegevens, dan kunnen zij gebruik maken van de verschillende communicatiekanalen die de Rechtspraak aanbiedt, zoals Facebook, Twitter, Instagram en Whatsapp. Daarnaast is het ook mogelijk om de FG te benaderen via functionarisgegevensbescherming@rechtspraak.nl.
Ambitieniveau: 5	Met de aanschaf van SmartPIA ontstaat een meer structureel proces om privacy te borgen. Dit zal er ook voor zorgen dat de gepubliceerde informatie op basis van de PDCA-cyclus steeds zal worden bijgewerkt.

8. Rechten van betrokkenen

Net als transparantie heeft dit hoofdstuk ook betrekking op de uitoefening van de rechten die de privacywet- en regelgeving betrokkenen toekend. Het hoofdstuk gaat in op de KPI die waarborgt dat verwerkingsverantwoordelijke adequaat en tijdig acteren op verzoeken van betrokkenen.

12. Faciliteren van en informeren over rechten van betrokkenen	
Norm	De organisatie reageert adequaat en tijdig op verzoeken van betrokkenen die hun privacyrechten willen effectueren.
Referentie	Artikel 12 t/m 23 AVG Artikel 17 t/m 26 Wjsg
Beoordeling	
Kwaliteitsniveau: 5	De privacywet- en regelgeving bieden rechtszoekenden en professionals de mogelijkheid om bepaalde rechten uit te oefenen. Het gaat dan bijvoorbeeld om recht op inzage, het recht van rectificatie en het recht om vergeten te worden. Om deze rechten te faciliteren is op rechtspraak.nl/privacy een procedure gepubliceerd waaruit blijkt hoe betrokkenen van hun rechten gebruik kunnen maken. Voor interne medewerkers geldt in beginsel dezelfde procedure. De procedures zijn ingevoerd binnen de Rechtspraak. Deze formulieren moet op basis van recente ervaringen worden geactualiseerd. Hier heeft de landsadvocaat ook op gewezen. Rechtszoekenden, professionals en andere betrokkenen moeten de wettelijke toegekende rechten ook kunnen uitoefenen indien persoonsgegevens namens de Rechtspraak door een derde partij worden verwerkt. Om dit te borgen bepaalt artikel 8 van de standaardverwerkersovereenkomsten (behorende bij de ARBIT en ARVODI) dat de wederpartij zal ondersteunen bij de uitvoering van de rechten van betrokkenen. In dezelfde template wordt steeds opgenomen wie de wederzijdse contactpersonen zijn. Tot slot is het bureau Raad in gesprek met ketenpartners om gezamenlijk af te spreken hoe wordt omgegaan met inzageverzoeken waarover meerdere organisaties moeten beslissen.
Ambitieniveau: 5	Met ketenpartners wordt onderzocht hoe invulling kan worden gegeven aan inzageverzoeken die betrekking hebben op meerdere organisaties in de keten (FG, Q4 2022). Daarnaast moet het aanvraagformulier op rechtspraak.nl/privacy worden herzien (FG/ adviseur privacy & informatiebeveiliging, Q4 2022) Er zijn geen signalen dat er op dit punt op korte termijn nog acties ondernomen dienen te worden.

9. Bewustzijn omtrent privacy en opleiding

Privacybewustzijn houdt in dat medewerkers binnen de Rechtspraak weten hoe ze met persoonsgegevens moeten omgaan. Dit betekent dat in alle gevallen binnen de gestelde beveiligingskaders wordt gehandeld. Mocht toch onverhoopt iets fout gaan, dan weten medewerkers hoe te handelen, zodat de organisatie recht doet aan de eisen uit de privacywet- en regelgeving en de impact voor betrokkenen zo klein mogelijk wordt gehouden. Het is de verantwoordelijkheden van de gerechten en de landelijke diensten om medewerkers hierin op te leiden en hiervan bewust te maken.

13. Bewustzijn omtrent privacy en opleiding	
Norm	De organisatie bevordert het privacybewustzijn van medewerkers
Referentie	Artikel 5 AVG Artikel 1 t/m 7 Wjsg
Beoordeling	
Kwaliteitsniveau: 2	Het privacybewustzijn wordt op landelijk en lokaal niveau bevorderd. Zo wordt op Intro landelijk regelmatig een bericht geplaatst in het kader van privacy of informatiebeveiliging. Daarnaast bevat de pagina jij-bent-de-sleutel informatie over het omgaan met persoonsgegevens en het handelen bij datalekken. Op lokaal niveau wordt in introductieprogramma's uitgebreid verteld over de wijze waarop met persoonsgegevens moet worden omgegaan en hoe moet worden gehandeld in geval van een datalek. Hierbij wordt gebruik gemaakt van het leaflet datalekken. In het algemeen kan worden geconstateerd dat het privacybewustzijn toeneemt, omdat medewerkers stellen steeds vaker privacyvragen stellen. Aan de andere kant gebeurt nog veel onder de radar en is er weinig inzicht in de daadwerkelijke mate van privacybewust zijn.
Ambitieniveau: 3	Hiervoor is in het kader van privacy by design en privacy by default al aan bod gekomen dat het privacybewustzijn moet worden vergroot, zodat voorafgaand aan een verwerking met de eisen uit de privacywet- en regelgeving rekening wordt gehouden. Tegelijkertijd moet duidelijk worden wat het niveau van privacybewustzijn is en moet een bewustwordingsstrategie worden ontwikkeld die past bij de Rechtspraak. Dit is ook vereist vanuit de BIO. In het kader van het laatstgenoemde is waardevol op te merken dat IVO werkt aan een systeem dat kan helpen bij de bewustwording. De leden van het SBO hebben aangegeven dat ze bij de landelijke implementatie van dit systeem gezamenlijk willen optrekken. Dat zal plaatsvinden als IVO positieve ervaringen heeft met het systeem.

10. Overig

In dit afsluitende hoofdstuk staan verschillende onderwerpen die aandacht behoeven, maar niet passen binnen de toetsingskaders van de privacymanagement KPI's en ook niet groot genoeg zijn voor een eigen KPI, zoals KPI 10.

Verwerking van personeelsgegevens

Door de HRM-afdelingen, Inkoop en externe onderzoekers binnen de Rechtspraak worden veel (vertrouwelijke) persoonsgegevens verwerkt. Het is van belang dat deze gegevens rechtmatig worden verzameld, rechtmatig worden verwerkt en tijdig worden verwijderd.

Naar aanleiding van signalen dat persoonsgegevens onveilig worden verstuurd, is het van belang om hier extra aandacht aan te besteden. Door de beleidsadviseur privacy en de FG is hierover gesproken met de manager HRM&OO. Naar aanleiding van dat overleg is aan een stuk over de functioneringsgesprekken RM toegevoegd dat met het oog op de AVG de verslagen van functioneringsgesprekken op basis van een periodieke risico-inschatting op een passende niveau moeten worden beveiligd.

Verder is privacy in de HR-processen een verantwoordelijkheid van ieder gerecht. De mate waarin privacy en AVG binnen de HR-processen daadwerkelijk aandacht krijgen, verschilt. Daarom is in de vakgroep HR expliciet aandacht gevraagd voor de privacy-aspecten. Op termijn beoogt de vakgroep HR samenwerkingsruimtes op te zetten waarin de leden van de vakgroep kennis kunnen delen over de wijze waarop met privacy binnen de HR-afdelingen wordt omgegaan.

Externe onderzoeken

Bij aanvragen van externe onderzoekers (zoals het WODC, CBS en universiteiten) wordt vaak verzocht om persoonsgegevens in dossierstukken en uitspraken. Het informatieprotocol bepaalt hoe met deze verzoeken moet worden omgegaan. Veelal ontbrak echter een privacytoets. Bij de herziening van het informatieprotocol worden daarom door de FG en de adviseur privacy & informatiebeveiliging voorstellen gedaan om de borging van privacy een plek te geven in het informatieprotocol.

Verder wordt in dit kader een werkgroep opgericht om aanvragen met betrekking tot externe onderzoeken in relatie tot privacy meer te stroomlijnen. In de loop van het jaar worden ontwikkelingen op dit punt verwacht.

SmartPIA

Deze nieuwe tool wordt op verschillende plekken in het borgingsplan genoemd vanwege de kansen die het systeem biedt voor privacymanagement. Op 26 mei is het implementatietraject gestart met een kick-off in Utrecht. Sinds 7 oktober 2021 zijn wekelijks sessies om overeenstemming te bereiken binnen het privacyteam over de inrichting en functionaliteiten van het systeem.

De verwachting is dat het systeem in februari gereed is voor het eerste gebruik. Geselecteerde collega's van de IVO Rechtspraak en het bureau Raad kunnen dan ervaring opdoen met het systeem. Deze ervaringen zullen nog tot de nodige aanpassingen leiden. Op een nog te bepalen moment wordt SmartPIA breder beschikbaar gesteld. Tot slot wordt moet de reeds uitgevoerde PIA's in het systeem worden ingevoerd.

Deelbesluit 1 - Datalekken
Document 14

datum	21 april 2022
datum overleg	20 april 2022
aanwezig	Olav Welling, [redacted]
Afwezig	[redacted]

Verslag werkgroep privacy 20 april 2022

1. Opening/mededelingen
   a. Statusupdate adresseringsfouten digitale postkamer
   Bijgevoegde stuk ter informatie
   [redacted] geeft een terugkoppeling over de ontwikkelingen met betrekking tot de adresseringsfouten digitale postkamer. Door het LOBRO is onderzoek gedaan naar de oorzaak van de adresseringsfouten. De conclusies hiervan zijn opgenomen in een notitie. Door aanvullende maatregelen zijn de aantallen aanzienlijk omlaag gegaan. De fouten die nu nog plaatsvinden worden veroorzaakt door nieuwe medewerkers die foutmeldingen negeren. De gerechten krijgen dagelijks een uitdraai van de fouten die de dag ervoor zijn gemaakt, zodat zij deze kunnen herstellen en hiervan melding kunnen doen.

   b. Uitwisselmap G-schijf
   In het vorige overleg is hierover gesproken. Toen is afgesproken dat een analyse van het probleem zou worden uitgevoerd. Op basis van die probleemanalyse worden dan vervolgacties bepaald. Een analyse van het probleem incl. oplossingen is naar de leden van de werkgroep toegestuurd. Tegelijkertijd wordt door [redacted] en [redacted] in opdracht van [redacted], een onderzoek uitgevoerd om inzicht te krijgen in de behoefte aan, en het gebruik van, opslag- en samenwerkingsvoorzieningen voor ongestructureerde data binnen de Rechtspraak. Dit onderzoek moet leiden tot aanbevelingen.

   In de werkgroep wordt afgesproken dat dit punt in het borgingsplan wordt opgenomen. [redacted] onderzoekt verder of dat bepaalde maatregelen nu al doorgevoerd kunnen worden of dat het beter is om de resultaten van het onderzoek af te wachten.

2. Vaststellen verslag 16 februari 2022
   Het verslag wordt zonder inhoudelijke wijzigingen aangenomen.

3. SmartPIA ([redacted])
   Voortgang wordt nog steeds geboekt. Inrichting voor de Rechtspraak als geheel is initieel gereed. Ook dashboard actief. Wordt nu ingericht. Deze week live gegaan met de hele uitvraag. Bestaande PIA's vastleggen in SmartPIA. Hierdoor blijkt dat ze niet altijd volkomen zijn om antwoord te geven op vragen die vanuit privacyperspectief interessant zijn. Leert veel over de PIA als tool. Iedereen is penvoerder en reviewer. Uiteindelijk wordt iedereen in het privacyteam reviewer.

Leverancier zo ver gekregen om binnen de bestaande kaders een oneindig aantal accounts te krijgen. Dat betekent dat iedereen nu zelf de PIA's kan gaan invoeren. [redacted] zal als een van de eerste gaan uitproberen. Dit past in de operationaliseringsstappen.

Hoe gaat het met de bekendheid binnen de Rechtspraak. Morgen in het LOBRO en uitleggen hoe we de gerechten kunnen aansluiten. Laten zien dat privacy daar niet anders is als voor IVO. Ieder kan daarbinnen z'n eigen ding doen binnen z'n eigen wereld. SmartPIA biedt dan eenduidig inzicht in de dingen die je wilt weten. Dat biedt eenduidige rapportage mogelijkheden met het oog op de informatiebehoefte.

Hoe gepresenteerd naar bestuurders, want nu nog onder de radar? Moeten we daar meer aan doen om te laten zien dat met dit instrumenten privacy makkelijker wordt. Het is sowieso gemakkelijker. Helpt je met het realiseren van de juiste normen en waarden t.a.v. privacy.

Volgens [redacted] voldoende aandacht besteed voor de collega's bij IVO. Eerste verzoeken zijn binnengekomen op PIA's te doen mbv SmartPIA.
Kunnen we na het uitvoeren van enkele PIA's de aura van complexiteit mbv SmartPIA wegnemen. Door te laten zien dat we handvatten hebben.

[redacted] we zijn een standaard training aan het ontwikkelen voor SmartPIA waardoor privacy ook als minder complex gezien moet gaan worden..

4. Herziening Richtlijn 2016/680 ([redacted]
    a. Degenen die bij de herziening van de Wjsg en de Wpg betrokken waren hebben bericht ontvangen dat het traject is gestopt. De Wpg wordt echter wel nog herzien, omdat daarvoor apart geld is gereserveerd.
    b. Het OM heeft in de Permanente Vergadering een pleidooi gehouden om Richtlijn 2016/680 op enkele punten aan te passen. Dit heeft ervoor gezorgd dat het OM op 6 mei 2022 de Europese Commissie mag gaan informeren. Vanuit de Rechtspraak en andere justitiepartijen wordt onderzocht hoe het OM bij de voorbereiding het beste kan worden ondersteund.

5. AVG-notitie en risicowerkgroep privacy
[redacted] heeft de stukken die IVO Rechtspraak heeft ingebracht voor de Raadsvergadering naar de leden van de werkgroep toegestuurd. De stukken betreffen de aanpak van IVO Rechtspraak om de systemen in lijn met de AVG/Wjsg te brengen. [redacted] is aangesloten om toelichting te geven op de stukken. De richting in de stukken is goed. Het vergt echter nog enige vasthoudendheid om alles wat in de stukken staat te realiseren en te monitoren.

Tijdens de Raadsvergadering van 13 april is ook het borgingsplan besproken. Helaas zijn de ambitieniveaus niet besproken. De Raad zal bij de volgend actualisatie van het borgingsplan hier nogmaals op worden geattendeerd.

5.2 [redacted]

[redacted] geeft aan dat het van belang is dat een werkgroep risicobeheersing bij elkaar komt om te bespreken hoe de actiepunten worden opgepakt. Het is van belang stop met achteruit kijken, maar gaat kijken naar de toekomst. [redacted] geeft aan dat een werkgroep in oprichting is en dat hij vanuit het bureau Raad zal aansluiten. Naast [redacted] zullen aansluiten: [redacted]. [redacted] wenst ook aan te sluiten. [redacted] geeft dit door

[redacted] houdt Olav op de hoogte over de ontwikkelingen van de werkgroep.

6. Voortgang acties E-archief

Eind vorig jaar zijn in het PRO afspraken gemaakt ten aanzien van het E-archief. 5.2 [redacted] Een van de actiepunten was de herbeoordeling van de uitgegeven autorisaties. Bij het bureau Raad loopt dit onderwerp, maar een monitoringsrapportage over de gehele Rechtspraak is nog niet ingezien. Daarnaast zou er een werkgroep van rechters en IVO- worden opgericht om de verbeterpunten gezamenlijk op te pakken. Ook ten aanzien van deze werkgroep heeft Olav nog geen bericht ontvangen.

Volgens [redacted] is die werkgroep er niet gekomen. [redacted] geeft aan dat de werkgroep eenmalig bij elkaar is gekomen om acties uit te zetten. Daarna is er geen vervolg mee geweest.

[redacted] geeft aan dat wordt gewerkt aan een nieuwe privacyverklaring voor het E-archief.

Verder vraagt Olav of er beleid inzake het toekennen van autorisaties (in E-archief) is. Dit is niet het geval. Het toekennen van autorisaties is een proces dat verloopt tussen degene die vraagt en degene die toekent. De vragen moet gronden geven, maar het is aan de leidinggevende om die gronden te toetsen. Uit de COR digicie bleek dat ondertussen weer autorisaties buiten het eigen rechtsdomein worden toegekend.

In relatie tot het vorige onderwerp wordt nog opgemerkt dat het E-archief buiten scope van de AVG-notitie is geplaatst, omdat hiervoor een apart traject loopt. [redacted] geeft aan dat hij dat niet begrijpt, omdat het nog steeds een systeem onder beheer van IVO is dat in lijn met de AVG/Wjsg moet worden gebracht. De voortgangsbewaking uit de werkgroep risicobeheersing zou ook een goede optie zijn om inzicht te geven in ontwikkelingen t.a.v. het E-archief.

Olav vraagt of er in de PRO-notities stond t.a.v. van voortgangsbewaking. [redacted] bevestigt dit, maar houdt een slag om de arm. [redacted] stuurt [redacted] de notitie om te kijken hoe het beste kan worden geacteerd. Olav wil de IV portefeuillehouder informeren over een dergelijk gevoelig onderwerp.

7. Rondvraag
[redacted] onlangs is er een incident geweest bij een gerecht. Documenten zouden foutief naar de Belastingdienst (BD) zijn gestuurd. De BD is gevraagd de stukken te verwijderen, maar zij gaven aan dat niet te doen met het oog op de bevoegdheid van de FIOD. Daarom is via [redacted] contact opgenomen met de plv. FG van het ministerie van Financiën. Op hun aangeven is door de president van het betreffende gerecht een brief aan de directeur-generaal van de BD gestuurd. Deze week is de bevestiging binnengekomen dat de stukken zijn vernietigd.

5.1(2)h [redacted]

[redacted] geeft aan dat het geactualiseerd beleidskader JenV in de CIO-raad wordt besproken. [redacted] zal de stukken ter info naar de leden toesturen.

[redacted] deelt mee dat binnenkort een nieuwe KCD-uitvraag wordt uitgezet.

Tot slot geeft [redacted] aan dat hij een gesprek met Olav laat inplannen om te praten over verschillende EU-verordeningen.

8. Sluiting

Deelbesluit 1 - Datalekken
Document 15

Addendum Privacy Governance Rechtspraak - Verdere uitwerking TBV

Inleiding

In de Privacy Governance Rechtspraak wordt de verdeling van verantwoordelijkheden ten aanzien van privacy op hoofdlijnen uitgewerkt. In de dagelijkse werkzaamheden zijn deze echter niet volledig. Wie doet bijvoorbeeld de melding bij een betrokkene als er een (grootschalig) datalek is bij IVO? En wie is er eindverantwoordelijk in het geval van een keten PIA?

Dit document is op 16 februari 2021 goedgekeurd door de Werkgroep privacy.

Doel

In dit document wordt de privacy governance beschreven en vastgelegd. Per taak wordt de eindverantwoordelijkheid aangevuld met adviserende, geïnformeerde en uitvoerende rollen. Hiermee worden de onderlinge verantwoordelijkheden op tactisch en operationeel niveau verduidelijkt. Met dit overzicht is de Rechtspraak in staat bevoegdheden te mandateren.

Uitgangspunt

- Het document maakt integraal onderdeel uit van de Privacy Governance Rechtspraak.
- Dit document tast uitwerkingen van verantwoordelijkheden in andere documenten niet aan.
- Ten aanzien van de eindverantwoordelijkheid:
    - De eindverantwoordelijke is de verwerkingsverantwoordelijke in de zin van de AVG en de Wet justitiële en strafvorderlijke gegevens
    - bij een lokale taak gaat het v.w.b. de eindverantwoordelijkheid om de gerecht/dienst waar de taak plaatsvindt. Hier is dus sprake van een 'of' relatie.
    - Bij een gerechtsoverstijgende taak is sprake van een 'en' relatie (gezamenlijk verantwoordelijk)
- De (IT-)governance is leidend in het bepalen van de onderverdeling tussen gerechtsbestuur c.q. directie en het bestuurs- c.q. directielid dat privacy in portefeuille heeft.
- Team Recht & ICT wordt afhankelijk van de casus betrokken.
- De taken en verantwoordelijkheden zijn niet altijd onverkort van toepassing. Dit zal veelal afhangen van de casus.
- De rol ‘business’ is bewust breed gekozen, omdat de uitvoering erg afhankelijk is van de context. In het projectverband liggen bepaalde verantwoordelijkheden bij een projectgroep. Daarnaast wordt de uitvoering verdeeld over verschillende personen en rollen. Zo kunnen ook degene die primair een adviserende taak hebben, uitvoerende taken hebben. Op gerechts- of dienstenniveau kan hier verder invulling aan worden gegeven.

Afkortingen van actoren

Adviseur IB&P	Adviseur informatiebeveiliging & privacy
CIO	Chief information officer

CISO	Chief information security officer
FG	Functionaris Gegevensbescherming, inclusief diens plaatsvervanger(s)
LOV	Landelijk overleg vakinhoud

1. Privacy Impact Assessment

Een privacy impact assessment (kortweg: PIA) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Daarna kan de PIA gebruikt worden om maatregelen te kunnen nemen, zodat risico's worden verkleind en/of worden geaccepteerd.

Ten aanzien van de PIA moet onderscheid worden gemaakt in: PIA's die betrekking hebben op landelijke verwerkingen, PIA's die betrekking hebben op lokale verwerkingen en PIA's 'in de keten'. Met dit laatste wordt een PIA bedoeld waarbij een of meerdere ketenpartners betrokken zijn. In dit kader is vooral relevant wie bevoegd is (rest)risico's te accepteren.

PIA's voor landelijke verwerkingen

- Eindverantwoordelijk: de gerechtsbesturen en de Raad voor de rechtspraak gezamenlijk
- Adviserend: FG, Adviseur IB&P, CISO, Privacy office
- Geïnformeerd: LOV
- Uitvoerend: business

PIA's voor lokale verwerkingen

- Indien de PIA wordt uitgevoerd door een van de gerechten:
  - Eindverantwoordelijk: gerechtsbestuur
  - Adviserend: FG, privacycoördinator
  - Uitvoerend: business
- Indien de PIA wordt uitgevoerd door een van de landelijke diensten:
  - Eindverantwoordelijk: directie landelijke dienst
  - Adviserend: FG, security officer, privacy officer
  - Uitvoerend: business

PIA 'in de keten'

- Eindverantwoordelijk: gerechtsbesturen en de Raad voor de rechtspraak gezamenlijk
- Adviserend: FG, CISO, Privacy officer
- Geïnformeerd: Business
- Uitvoerend: Ketenpartners

2. Register van verwerkingsactiviteiten

De privacy- en regelwetgeving verplicht de verwerkingsverantwoordelijke verantwoordelijkheid af te leggen over de verwerking van persoonsgegevens. Hierin staat o.a. welke verwerkingen plaatsvinden, welke persoonsgegevens daarvoor worden verwerkt en hoelang de gegevens worden bewaard. Ieder gerecht en de landelijke dienst is verplicht lokaal een register bij te houden. Daarnaast is er op landelijk niveau een register voor verwerkingen die het gerecht en/of de landelijke dienst overstijgen.

Landelijk register van verwerkingsactiviteiten

- Eindverantwoordelijk: gerechtsbesturen en de Raad voor de rechtspraak gezamenlijk
- Geïnformeerd: FG, Adviseur IB&P
- Uitvoerend: Privacy officer, business

Lokaal register van verwerkingsactiviteiten

- Indien het een register betreft van een van de gerechten:
  - Eindverantwoordelijk: gerechtsbestuur
  - Geïnformeerd: FG, Adviseur IB&P
  - Uitvoerend: privacycoördinator, business

- Indien het een register van een landelijke dienst betreft:
  - Eindverantwoordelijk: Directie landelijke dienst
  - Geïnformeerd: FG, Adviseur IB&P
  - Uitvoerend: Privacy officer, privacycoördinator, business.

3. Datalekken

Bij een datalek is er sprake van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens

De meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) binnen 72 uur na kennisneming een melding moeten doen bij de toezichthouder[1] zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkene(n) (de persoon/personen van wie de persoonsgegevens zijn gelekt).

Bij dit onderdeel kan onderscheid worden gemaakt in de afhandeling van een incident of datalek, de melding aan de toezichthouder en de melding aan betrokkene. Binnen iedere categorie kan onderscheid worden gemaakt in een lokaal incident/datalek en een incident/datalek met landelijke impact.

[1] Afhankelijk van de aard van de verwerking gaat het om de procureur-generaal bij de Hoge Raad, de AVG-commissie of de Autoriteit Persoonsgegevens.

Afhandeling van een landelijk incident of datalek
- Eindverantwoordelijk: gerechtsbesturen en de Raad voor de rechtspraak gezamenlijk (veelal verenigd in het CMT)
- Adviserend: CIO, Beveiligingsambtenaar, FG, Adviseur IB&P, teamleider SP&K/CISO
- Geïnformeerd: Communicatie/persvoorlichter
- Uitvoerend: Portefeuillehouders IVO, Dienstenmanagers IVO, Incidentenmanagers, business

Afhandeling van een lokaal incident of datalek
- Indien het een incident/datalek betreft van een van de gerechten:
    - Eindverantwoordelijk: gerechtsbestuur
    - Geïnformeerd: FG
    - Adviserend: Adviseur IB&P, CISO/Teamleider SP&K, privacy officer
    - Uitvoerend: privacycoördinator, business

- Indien het een incident/datalek van een landelijke dienst betreft:
    - Eindverantwoordelijk: directie landelijke dienst
    - Geïnformeerd: CISO/Teamleider SP&K, communicatie/persvoorlichter, business
    - Adviserend: Adviseur IB&P
    - Uitvoerend: Portefeuillehouders IVO, Dienstenmanagers IVO, Incidentenmanagers, FG, Privacy officer, business

Melding van een landelijk datalek aan de toezichthouder
- Eindverantwoordelijk: directie landelijke dienst
- Geïnformeerd: CISO/Teamleider SP&K, communicatie/persvoorlichter, business
- Uitvoerend: FG, Privacy coördinator

Melding van een lokaal datalek aan de toezichthouder
- Indien het een datalek betreft van een van de gerechten:
    - Eindverantwoordelijk: gerechtsbestuur
    - Geïnformeerd: FG, Adviseur IB&P, communicatie/persvoorlichter
    - Uitvoerend: privacycoördinator, business

- Indien het een datalek van een landelijke dienst betreft:
    - Eindverantwoordelijk: directie landelijke dienst
    - Geïnformeerd: FG, Adviseur IB&P, CISO/Teamleider SP&K, communicatie/persvoorlichter
    - Uitvoerend: Privacy officer, privacycoördinator, business.

Informeren van betrokkene(n) over een landelijk datalek
- Eindverantwoordelijk: directie landelijke dienst
- Geïnformeerd: gerechtsbestuur, FG
- Uitvoerend: communicatie/persvoorlichter

Informeren van betrokkene(n) over een lokaal datalek

- Indien het een datalek betreft van een van de gerechten:
    - Eindverantwoordelijk: gerechtsbestuur
    - Geïnformeerd: FG, communicatie/persvoorlichter, business
    - Uitvoerend: privacycoördinator, business

- Indien het een datalek van een landelijke dienst betreft:
    - Eindverantwoordelijk: directie landelijke dienst
    - Geïnformeerd: FG, communicatie/persvoorlichter, business
    - Uitvoerend: Privacy officer, privacycoördinator

4. Beleid

Deugdelijk gedragen beleid is randvoorwaardelijk voor gegevensverwerking in lijn met de privacywet- en regelgeving. Het overkoepelend privacybeleid wordt op landelijk niveau op- en vastgesteld. Het beleid wordt gedragen door alle gerechten en diensten. Gerechten en landelijke diensten kunnen op lokaal niveau verder invulling geven aan het overkoepelende beleid aan de hand van richtlijnen en werkinstructies.

Bij dit onderdeel wordt een onderscheid gemaakt in landelijk (overkoepelend) beleid en lokaal beleid.

Landelijk beleid

- Eindverantwoordelijk: gerechten en Raad voor de rechtspraak gezamenlijk
- Adviserend: FG, Team Recht & ICT, CISO/ Teamleider SP&K, Privacy officer
- Geïnformeerd: privacy coördinator, ketenpartners, LOV's, Business
- Uitvoerend: Adviseur IB&P

Lokaal beleid

- Indien het beleid bij een gerecht wordt opgesteld:
    - Eindverantwoordelijk: gerechtsbestuur
    - Adviserend: FG, Adviseur IB&P
    - Uitvoerend: privacycoördinator

- Indien het beleid bij een landelijk dienst wordt opgesteld:
    - Eindverantwoordelijk: directie landelijke dienst
    - Adviserend: FG, Adviseur IB&P, CISO/Teamleider SP&K
    - Uitvoerend: Privacy officer, privacycoördinator

5. Verbintenissen met partijen

Veelvuldig komt het voor dat met externe partijen privacyovereenkomsten afgesloten moeten worden over de verdeling van privacyverantwoordelijkheden. Dit worden privacyafspraken of

verwerkersovereenkomsten genoemd. Op lokaal en landelijk niveau kunnen deze overeenkomsten worden afgesloten.

Landelijke overeenkomst

- Eindverantwoordelijk: gerechten en Raad voor de rechtspraak gezamenlijk
- Adviserend: FG, Adviseur IB&P, Privacy officer
- Uitvoerend: Contractmanager IVO/ LDCR inkoop, business

Lokale overeenkomst

- Indien de overeenkomst bij een gerecht wordt opgesteld:
  - Eindverantwoordelijk: gerechtsbestuur
  - Adviserend: FG, privacycoördinator
  - Uitvoerend: Contractmanager IVO/ LDCR inkoop

- Indien de overeenkomst bij een landelijk dienst wordt opgesteld:
  - Eindverantwoordelijk: directie landelijke dienst
  - Adviserend: FG, Privacy officer, privacycoördinator
  - Uitvoerend: Contractmanager IVO/ LDCR inkoop

6. Overig

Naast de bovengenoemde onderwerpen brengt de privacywet- en regelgeving nog andere verplichtingen mee, die niet onder één noemer zijn samen te vatten. Het gaat dan bijvoorbeeld om klachten en informatieverzoeken, de besluitvorming inzake de doorgifte van persoonsgegevens naar derde landen en deugdelijk beheer van persoonsgegevens. Deze verplichtingen worden gezien hun diversiteit hieronder verder uitgewerkt.

Klachten en verzoeken

De privacywet- en regelgeving geeft een betrokkene de bevoegdheid om een klacht in te dienen bij de toezichthoudende autoriteit over de verwerking van persoonsgegevens door de Rechtspraak. Daarnaast kan betrokkene diverse verzoeken indienen die betrekking hebben op zijn persoonsgegevens. Het gaat dan om inzageverzoeken, wijzigingsverzoeken, verwijderverzoeken en verzoeken om de gegevensverwerking te beperken.

Een klacht of een informatieverzoek heeft alleen betrekking op lokale verwerkingen. De verantwoordelijkheden, taken en bevoegdheden zijn dan als volgt verdeeld:

Lokale klacht of verzoek

- Indien de klacht of het verzoek bij een gerecht wordt ingediend:
  - Eindverantwoordelijk: gerechtsbestuur
  - Adviserend: FG, Adviseur IB&P, privacycoördinator
  - Uitvoerend: Klachtenfunctionaris/coördinator informatieverzoeken

- Indien de klacht of het verzoek bij een landelijk dienst wordt ingediend:
  - Eindverantwoordelijk: directie landelijke dienst
  - Adviserend: FG, Adviseur IB&P
  - Uitvoerend: Klachtenfunctionaris/ coördinator informatieverzoeken

Indien meerdere gerechten en/of diensten eenzelfde informatieverzoek ontvangen, zal de Adviseur IB&P een coördinerende rol vervullen conform de betreffende procedure. Deze coördinerende rol laat de verantwoordelijkheden van de gerechten en diensten onverlet.

Doorgifte naar derde landen (incl. Aruba, Sint-Maarten, Curaçao en de BES-eilanden)
Derde landen zijn landen die niet onder de werking van de privacywet- en regelgeving vallen. Het gaat dan om de landen buiten de Europese Economische Ruimte. Van doorgifte spreekt men indien de persoonsgegevens van de Rechtspraak naar derde landen worden verstuurd en in die landen worden verwerkt. Hierover moet steeds een weloverwogen beslissing worden genomen.

- Eindverantwoordelijk: gerechten en de Raad voor de rechtspraak gezamenlijk
- Adviserend: FG, Adviseur IB&P, CISO/Teamleider SP&K, Privacy officer
- Uitvoerend: directie landelijke dienst (veelal IVO Rechtspraak), business

Vernietiging en archivering van data
Een van de beginselen van de privacywet- en regelgeving is dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is. Na de inzichtelijk te maken moeten de persoonsgegevens vernietigd of gearchiveerd worden. Het is van belang dat duidelijk hoe de taken, bevoegdheden en verantwoordelijkheid verdeeld zijn. Dit waarborgt dat persoonsgegevens tijdig worden vernietigd of worden gearchiveerd.

- Eindverantwoordelijk: Gerechten en Raad voor de rechtspraak gezamenlijk
- Geïnformeerd: LOV's
- Adviserend: FG, Adviseur IB&P, Privacy officer
- Uitvoerend: Dienstenmanager IVO, Ketenpartners, archivarissen en de business.

Aanpassen van systemen
De stand van de techniek en het risicoprofiel (als gevolg van de maatschappelijke omgeving) veranderen continu. De verplichtingen uit de privacywet- en regelgeving staan dan ook niet stil. In lijn met de PDCA-cyclus is privacy een continu proces van verbetering. Dit brengt met zich mee dat de systemen van de Rechtspraak steeds moeten worden aangepast. Het is van belang om de verantwoordelijkheden duidelijk te hebben. De verantwoordelijkheden worden aangevuld door de IT-governance.

- Eindverantwoordelijk: Raad voor de rechtspraak
- Geïnformeerd: Adviseur IB&P
- Adviserend: FG, CISO, teamleider SP&K, Privacy officer,
- Uitvoerend: dienstenmanagers IVO, portefeuillehouders IVO

Wetgeving en Kamervragen
Privacywet- en regelgeving wordt periodiek herzien. Relevante wetgevingstrajecten die in dit kader te noemen zijn, zijn de Uitvoeringswet AVG, de Verzamelwet gegevensbescherming en het herzieningstraject Wet justitiële en strafvorderlijke gegevens en de Wet politiegegevens. Voor wetgevingstrajecten met een privacy component is het van belang te beschrijven hoe de verantwoordelijkheden zijn belegd en wie de coördinatie voert.

- Eindverantwoordelijk: Raad voor de rechtspraak
- Geïnformeerd: business
- Uitvoerend: Team Recht & ICT (coördinerend), LOV's, FG, Privacy Officer

Deelbesluit 1 - Datalekken
Document 16

D.5.01 Minimumnorm privacy

Documentbeheer

Documenteigenaar	[redacted]
Rubricering	Vertrouwelijk
Goedkeuring	Raad voor de rechtspraak
Geldig tot	01-09-2023
Soort document	Minimumnorm

Wijzigingshistorie			
Versie	Auteur	Datum	Toelichting
1.0	Team BVA	15-09-2020	Initiële opstelling

Doel, doelgroep en positionering

Deze minimumnorm:	waarborgt dat persoonsgegevens in lijn met het vigerende privacyregime worden verwerkt.
Bestemd voor:	Iedereen binnen de Rechtspraak met nadruk op de Privacycoördinatoren en andere privacyfunctionarissen binnen de Rechtspraak
Positie in het handboek:	

Inhoudsopgave

1 Inleiding

Achtergrond

Het (wettelijke) privacylandschap is sinds 25 mei 2018 aanzienlijk veranderd. Waar eerst de Wet bescherming persoonsgegevens de boventoon voerde, regelen de Wet justitiële en strafvordelijke gegevens en het bijbehorende besluit het privacyregime voor gegevens die worden verwerkt voor strafrechtelijke en justitiële doeleinden. Voor de verwerking van persoonsgegevens voor andere doeleinden wordt het privacyregime door de (Europese) Algemene Verordening Gegevensbescherming en de bijbehorende (nationale) Uitvoeringswet gevormd.

De genoemde privacywet- en regelgeving bevatten veel open normen die ruimte bieden voor interpretatie. Om hier invulling aan te geven, heeft de Rechtspraak een Strategisch Plan Privacy, een Privacy Governance en een Privacy Beleidsdocument opgesteld. Het uitgangspunt hierin is dat de Rechtspraak altijd voldoet aan de geldende wet- en regelgeving. Om hiervoor concrete handvatten te bieden is de minimumnorm privacy opgesteld.

De minimumnorm privacy is gebaseerd op het normenkader van het Centrum voor Informatiebeveiliging en Privacy (CIP). Nu dit kader zich primair richt op de AVG, is dit kader voor de Rechtspraak aangevuld met specifieke normen die op de Wjsg en het bijbehorende besluit zijn geënt.

Doelstelling

Deze minimumnorm beoogt de open normen in de privacywet- en regelgeving zo veel mogelijk te concretisering. Hierbij wordt rekening gehouden van de eigenheid van ieder gerecht c.q. landelijke dienst en verwerking.

Doelgroep

De minimumnorm is primair gericht aan de beveiligingscoördinatoren (BVC’ers) en privacy coördinatoren van de Rechtspraak. Privacy is echter niet een onderwerp dat bij een persoon hoort. Privacy wordt teruggevonden in alle aspecten van de dagelijkse werkzaamheden. Deze minimumnorm geldt daarom voor iedereen binnen de Rechtspraak.

Leeswijzer

In de navolgende hoofdstukken worden normen op basis van het normenkader van het CIP per onderwerp geclusterd. Per onderwerp zijn de Wjsg-normen toegevoegd. De oorsprong van een norm staat steeds naast de norm.

2 Doelbinding en rechtvaardigingsgronden

In de AVG, de UAVG en de Wjsg worden de beginselen opgenoemd die in acht genomen moeten worden bij het verwerken van persoonsgegevens.[1] Een van deze beginselen is doelbinding. Hiermee wordt bedoeld dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en vervolgens niet verder verwerkt mogen worden op een met die doeleinden onverenigbare wijze.[2]

Het doel van deze minimumnorm is om te waarborgen dat persoonsgegevens alleen worden verzameld en (verder) verwerkt voor gerechtvaardigde doeleinden. Hiermee wordt voorkomen dat ongeoorloofde en onrechtmatige verzameling en (verder) verwekring van persoonsgegevens plaatsvindt. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat.

'Welbepaald' houdt in dat deze doelomschrijving duidelijk moet zijn. De doelomschrijving moet tijdens het verzamelproces een kader bieden waaraan getoetst kan worden of de gegevens noodzakelijk zijn voor dat doel of niet.[3] Het doel mag niet in de loop van het verzamelproces geformuleerd worden. Dit moet voorafgaand zijn gedaan. 'Uitdrukkelijk omschreven' houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt moet hebben uitgelegd.

Daarnaast moet de gegevensverwerking rechtmatig zijn; dit vereist een grondslag op basis van artikel 6 AVG of art. 51f lid 1 jo. 3 lid 2 Wjsg.

In dit document wordt ingegaan op de normen voor:

- De doeleinden, en:
- De rechtvaardigingsgronden voor:
  a) verdere verwerking op grond van de verenigbaarheid met de oorspronkelijke gerechtvaardigde doeleinden;
  b) de geautomatiseerde besluitvorming;
  c) verwerking van bijzondere categorieën persoonsgegevens;
  d) verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten;
  e) verwerking van het nationaal identificerend nummer;
  f) verwerking van persoonsgegevens ten behoeve van wetenschappelijk of historisch onderzoek met een statistisch oogmerk en archivering in het algemeen belang.

[1] Artikel 5 AVG
[2] Artikel 5 lid 1b AVG
[3] Artikel 5 lid 1c AVG

2.1 Normen voor de doeleinden

Nummer	Norm	Referentie
PN 01-01	Het doel van de verwerking wordt vóórdat de gegevensverwerking begint vastgesteld. Tijdens het verzamel- of het verwerkingsproces wordt het doel niet vastgesteld of gewijzigd.	Art. 5 lid 1 en overweging 50 AVG
PN 01-02	Het doel is zodanig vastgesteld dat het een kader biedt waaraan getoetst kan worden of de gegevens noodzakelijk zijn voor het doel en bij verdere verwerking of de verwerking van de gegevens verenigbaar is met het oorspronkelijke doel.[4]	Art. 5 lid 1b AVG
PN 01-03	Gerechtelijke strafgegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens de Wjsg geformuleerde doeleinden en slechts voor zover deze te verwerken gegevens bij of krachtens de Wjsg als gerechtelijke strafgegevens zijn aangemerkt.	Art. 51f, lid 1 jo. 3 lid 2 Wjsg
PN 01-04	De persoonsgegevens en gerechtelijk strafgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.	Art. 3 lid 3 Wjsg en art. 5 AVG
PN 01-05	De verwerking van persoonsgegevens moet rechtmatig gebeuren. Hiervan is sprake wanneer aan een van de volgende voorwaarden is voldaan: a. De betrokkenen heeft toestemming gegevens voor de verwerking van zijn persoonsgegevens voor een of meerdere specifieke doelen[5]; b. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór sluiting van de overeenkomst maatregelen te nemen; c. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke; d. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen; e. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen; f. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde. Dat geldt niet wanneer de belangen of grondrechten en de fundamentele vrijheden van de betrokkene van wie de persoonsgegevens worden verwerkt zwaarder wegen. Dat geldt sowieso wanneer de betrokkene een kind is. Verder kan deze grondslag niet gebruikt worden door overheidsinstanties in het kader van de uitoefening van hun taak. Voor ‘typisch bedrijfsmatige handelingen’ geldt de grondslag wel.	Art. 6 lid 1 AVG
PN 01-06	Persoonsgegevens moeten behoorlijk en transparant worden verwerkt ten opzichte van de betrokkene.	Art. 5 AVG en art. 51f lid 1 jo. 3 Wjsg

[4] Gegevens mogen ook voor meerdere doelen verzameld en verwerkt worden. Voor al deze doelen afzonderlijk geldt dat ze tijdig moeten worden vastgesteld, gerechtvaardigd zijn en welbepaald en uitdrukkelijk zijn omschreven
[5] Zie verder Minimumnorm Privacy - Informatieverstrekking aan betrokkene.

2.2 Verdere verwerking

Nummer	Norm	Referentie
PN 01-07	De verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld is alleen mogelijk, wanneer: 1. de verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld en de verwerkingsverantwoordelijke bij de beoordeling van de verenigbaarheid onder meer rekening houdt met: a) Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking; b) Het kader waarin de persoonsgegevens zijn verzameld, met name wat betreft de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke; c) De aard van de persoonsgegevens, met name of bijzondere categorieën persoons- gegevens worden verwerkt en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt ; d) De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; e) Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering; of: 2. De verdere verwerking plaatsvindt op basis van de toestemming van betrokkene; of: 3. Wanneer de verdere verwerking berust op een wettelijke bepaling waarbij een specifieke uitzondering geldt.	Art. 25, 26 en 27 AVG
PN 01-08	Wanneer de verwerkingsverantwoordelijke zich een verdere verwerking voorneemt dan moet de verwerkingsverantwoordelijke de betrokkene nog vóór die verdere verwerking informatie over dat andere doel en andere noodzakelijke informatie verstrekken. Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld, omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt.	Overweging 61 AVG
PN 01-09	De verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt als verenigbaar met de oorspronkelijke doeleinden beschouwd	Overweging 50 AVG
PN 01-10	De verwerking voor een ander doel dan dat waarvoor de gerechtelijke strafgegevens zijn verzameld is alleen mogelijk, wanneer: 1. a. de Wjsg of een ieder verbindend besluit van de Europese Unie daar uitdrukkelijk in voorziet en; b. De verwerking niet onverenigbaar is met het doel waarvoor de gegevens zijn verkregen en; c. De verwerking voor dat andere doel noodzakelijk is en; d. De verwerking voor dat andere doel in verhouding staat tot dat doel en; 2. de verdere verwerking alleen mogelijk is door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang of in een bindend besluit van de Europese Unie zijn aangewezen	Art. 51f lid 1 jo. 3 lid 4 en 6 Wjsg

2.3 Bijzondere categorieën persoonsgegevens

Nummer	Norm	Referentie
PN 01-11	De verwerking van bijzondere categorieën persoonsgegevens is in beginsel niet toegestaan. Bij het verwerken van bijzondere persoonsgegevens gaat het om de verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Het verbod is niet van toepassing als aan een van de voorwaarden uit art. 9 lid 2 AVG is voldaan. De verschillende voorwaarden zijn hieronder verder uitgewerkt.	Art. 9 AVG
PN 01-12	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven	Art. 9 lid 2a AVG
PN 01-13	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke, op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt. Tevens geldt hierbij dat het verbod om gegevens over gezondheid te verwerken niet van toepassing is indien de verwerking geschiedt door werkgevers die te hunnen behoeve werkzaam zijn, en voor zover de verwerking noodzakelijk is voor: a) Een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene; of b) De re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid. Hierbij worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.	Art. 9 lid 2b AVG Art. 30 lid 1 UAVG Art. 30 lid 4 UAVG
PN 01-14	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven.	Art. 22 lid 2b UAVG; art. 9 lid 2c AVG
PN 01-15	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt.	Art. 22 lid 2d UAVG; Art. 9 lid 2e AVG

PN 01-16	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.	Art. 22 lid 2e UAVG; art. 9 lid 2f AVG
PN 01-17	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht. Hierbij gaat het voor de Rechtspraak om: 1. Nationaalrechtelijke algemene uitzonderingen: a) De verwerking is noodzakelijk ter voldoening aan een volkenrechtelijke verplichting; b) De verwerking is noodzakelijk in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt. 2. Uitzondering inzake verwerking van persoonsgegevens waaruit ras of etnische afkomst blijkt: a) Verwerking met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is; of 3. De verwerking biometrische gegevens: de verwerking vindt plaats ten behoeve van de unieke identificatie van een persoon, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Voor al deze verwerkingen is bepaald dat de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.	Art. 23 UAVG Art. 25 UAVG Art. 26 UAVG Art. 27 UAVG Art. 28 UAVG Art. 29 UAVG
PN 01-18 [6]	De verwerking van bijzondere categorieën van persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, waarbij: a) de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid, van de verordening; b) het onderzoek, bedoeld in onderdeel a, een algemeen belang dient; c) het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en d) bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.	Doeleinden overeenkomstig art. 89 lid 1 AVG Art. 9 lid j AVG Art. 24 UAVG Overweging 159 AVG
PN 01-19	De verwerking van gerechtelijke strafgegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke person, of gegevens over gezondheid, seksuele leven en seksuele gerichtheid vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en wanneer dit onvermijdelijk is voor het doel van de verwerking.	Art. 51h, lid 1 jo. 39c, lid 3 Wjsg

[6] Zie ook PN 01-29 en verder.

2.4 Strafrechtelijke veroordelingen en strafbare feiten

Dit hoofdstuk is alleen van toepassing indien de Rechtspraak taken moet uitvoeren waarvoor persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten noodzakelijk zijn, indien de doeleinden niet vallen onder de werking van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad. Bij de doeleinden van de Richtlijn gaat het om de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens. Dit hoofdstuk ziet op verwerking van strafrechtelijke gegevens voor andere doeleinden.

Nummer	Norm	Referentie
PN 01-20	Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt indien: a) De betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden; b) De verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven; c) De verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt; d) De verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;	Art. 32 UAVG
PN 01-21	Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (inclusief een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag) of daarmee verband houdende veiligheidsmaatregelen mogen worden verwerkt indien: a) De verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, alsmede door verwerkingsverantwoordelijken die deze hebben verkregen krachtens de Wet justitiële en strafvorderlijke gegevens (Wjsg); b) De verwerking geschiedt door en ten behoeve van publiekrechtelijke samenwerkings- verbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoor- delijken, indien: 1. De verwerking noodzakelijk is voor de uitvoering van de taak van deze verwerkings- verantwoordelijken of groepen van verwerkingsverantwoordelijken; en 2. Bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad; of c) De verwerking noodzakelijk is in aanvulling op de verwerking van gegevens over gezondheid, bedoeld in de UAVG art. 30, derde lid, aanhef en onderdeel a, met het oog op een goede behandeling of verzorging van de betrokkene; d) Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkings- verantwoordelijke die deze gegevens ten eigen behoeve verwerkt: 1. Ter beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren, of:	Art. 33 UAVG

	Ter bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn;	

2.5 Nationaal identificerend nummer

Nummer	Norm	Referentie
PN 01-22	Het verwerken van een nummer dat ter identificatie van een persoon bij wet is voorgeschreven wordt slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden die bij de wet zijn bepaald: • Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer (BSN), zonder dat daarvoor nadere regelgeving vereist is.	Art. 46 UAVG

2.6 Geautomatiseerde besluitvorming

Nummer	Norm	Referentie
PN 01-23	Een betrokkene wordt niet onderworpen aan een geautomatiseerde individuele besluitvorming, tenzij het besluit is toegestaan bij de wet- en regelgeving die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene.[7]	Art. 22 lid 1 en 2 AVG Art. 40 lid 3 UAVG
PN 01-24	Indien geautomatiseerde besluitvorming plaatsvindt, treft de verwerkingsverantwoordelijke passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.	Art. 22 lid 3 AVG
PN 01-25	De betrokkene wordt de logica meegedeeld die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.	Art. 13 lid 2f AVG
PN 01-26	Een besluit dat uitsluitend op geautomatiseerde verwerking is gebaseerd, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, is verboden, tenzij: a) Het besluit voorziet in het recht op menselijke tussenkomst van de zijde van de verwerkingsverantwoordelijke en b) wordt voorzien in specifieke voorlichting aan de betrokkene.	Art. 51f, lid 1 jo. 7e lid 1 Wjsg
PN 01-27	Een besluit als bedoeld onder PN 01-26 wordt niet gebaseerd op bijzondere categorieën van gerechtelijke strafgegevens, tenzij a) passende maatregelen zijn getroffen ter bescherming van de rechten en vrijheden en van de gerechtvaardigde belangen van de betrokkene.	Art. 51h, lid 1 jo. 39c, lid 4 Wjsg
PN 01-28	Profilering die leidt tot discriminatie van personen is verboden.	Art art. 51f lid 1 jo. 7e lid 2 Wjsg

[7] Het begrip 'besluit' in de zin van de AVG dient hierbij ruimer te worden gelezen dan het besluitbegrip uit de Awb; ook private partijen vallen onder de reikwijdte van deze bepaling wanneer ze gebruik maken van geautomatiseerde besluitvorming.

2.7 Wetenschappelijk of historisch onderzoek met een statistisch oogmerk

Nummer	Norm	Referentie
PN 01-29	De verwerking van bijzondere categorieën persoonsgegevens ten behoeve van wetenschappelijk onderzoek of statistiek en archivering in het algemeen belang vindt plaats voor zover deze aan de vereisen uit PN 01-18 voldoen.	art. 24 UAVG art. 9 lid 2j AVG
PN 01-30	Verwerking van persoonsgegevens ten behoeve van wetenschappelijk onderzoek of archivering vindt alleen plaats, als passende technische en organisatorische maatregelen zijn getroffen om de rechten en vrijheden van de betrokkene te beschermen door: • minimale gegevensverwerking te garanderen; • zorg te dragen dat de betrokkene niet meer geïdentificeerd kan worden, bijvoorbeeld door middel van pseudonimisering of anonimisering.	art. 5 lid 1e AVG
PN 01-31	Gerechtelijke strafgegevens kunnen slechts worden verstrekt ten behoeve van beleidsinformatie, wetenschappelijk onderzoek en statistiek nadat aan de betrokken onderzoeker daartoe schriftelijk toestemming is verleend door tussenkomst van het bestuur van een gerecht, bedoeld in artikel 2 van de Wet op de rechterlijke organisatie, dat voor die gegevens verwerkingsverantwoordelijke is.	Art. 15 Wjsg jo. art. 31 lid 2 Bjsg
PN 01-32	De toestemming genoemd in PN 01-31 wordt slechts gegeven indien: a. de beleidsinformatie of het onderzoek het algemeen belang dient; b. de organisatie die de gegevens verstrekt niet onnodig wordt belast; c. de beleidsinformatie zonder de betrokken gegevens onvolledig is of het onderzoek zonder de betrokken gegevens niet kan worden uitgevoerd, en d. de persoonlijke levenssfeer van de betreffende personen niet onevenredig wordt geschaad. Aan de toestemming, bedoeld in het eerste of tweede lid, kunnen voorwaarden worden verbonden.	Art. 31 lid 3 Bjsg

3 Register van verwerkingsactiviteiten

Om naleving met de privacywet- en regelgeving aan te tonen, dienen verwerkersverantwoordelijken en verwerkers een register van verwerkingsactiviteiten bij te houden die onder zijn verantwoordelijkheid hebben plaatsgevonden. Desgevraagd moeten de gerechten en de Raad voor de rechtspraak het register aan de toezichthoudende autoriteit verstrekken met het oog op het toezicht op de verwerkingsactiviteiten.[8]

Het doel van het register van verwerkingsactiviteiten is inzicht te geven in de verwerking en de gegevensstromen binnen de organisatie en bij de partijen die namens de organisatie zorgen voor de verwerking van persoonsgegevens. Ontbreken van een (volledig) register leidt tot een incompleet beeld van de verwerkte categorieën en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.

[8] Overweging 82 AVG

3.1 Register

Nummer	Norm	Referentie
PN 02-01	Elk gerecht en landelijke dienst houdt een register van verwerkingsactiviteiten bij die onder hun verantwoordelijkheid plaatsvinden.[9] IVO Rechtspraak houdt in het landelijk register de verwerkingen bij die plaatsvinden in de landelijke systemen.	Art. 30 lid 1 AVG Art. 51h lid 1 jo. 26c Wjsg
PN 02-02	Het register van verwerkingsactiviteiten van de verwerkingsverantwoordelijke bevat alle volgende gegevens: 1. De naam en de contactgegevens van: a) De verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en: b) In voorkomend geval: i. Van de vertegenwoordiger van de verwerkingsverantwoordelijke, en: ii. Van de Functionaris voor gegevensbescherming; 2. De verwerkingsdoeleinden; 3. Een beschrijving van de categorieën van betrokkenen; 4. Een beschrijving van de categorieën persoonsgegevens; 5. De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt; 6. Bij doorgiften aan een derde land of een internationale organisatie: a) De doorgifte van verstrekte persoonsgegevens b) De vermelding van dat derde land of die internationale organisatie c) De documenten inzake de passende waarborgen; 7. De beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist (indien mogelijk); 8. Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (indien mogelijk). 9. in voorkomend geval; het gebruik van profilering 10. een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de gerechtelijke strafgegevens bedoeld zijn.	Art. 30 lid 1 AVG Art. 51h lid 1 jo. 26c lid 1 Wjsg
PN 02-03	Indien een onderdeel van de Rechtspraak als verwerker verwerkingen uitvoert voor een partij buiten de Rechtspraak, bevat het register van de verwerker met alle categorieën van verwerkingsactiviteiten alle volgende gegevens: 1. De naam en de contactgegevens van: a) De verwerkers b) Iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt. In voorkomend geval: i. De vertegenwoordiger van de verwerkingsverantwoordelijke, of: ii. De verwerker en de Functionaris voor gegevensbescherming; 2. De categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd; 3. Bij doorgiften aan een derde land of een internationale organisatie: a) De doorgifte van verstrekte persoonsgegevens b) De vermelding van dat derde land of die internationale organisatie c) De documenten inzake de passende waarborgen; 4. Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (indien mogelijk).	Art. 30 lid 1 AVG Art. 51h lid 1 jo. 26c lid 2 Wjsg
PN 02-04	Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.	Art. 30 lid 3 AVG

[9] Een landelijke dienst houdt het register bij namens de Raad voor de rechtspraak

PN 02-05	Op verzoek van de toezichthouder wordt het register beschikbaar gesteld.	Art. 30 lid 4 AVG

4 Datakwaliteit en rechten van betrokkene

Voor de Rechtspraak en voor betrokkenen is het van belang dat persoonsgegevens correct en ter zake dienend zijn. Onjuiste of onnauwkeurige gegevens kunnen zorgen voor verkeerde conclusies met eventueel negatieve consequenties tot gevolg of ongewenste verwerking van persoonsgegevens van betrokkenen. Het verwerken van persoonsgegevens die niet noodzakelijk zijn om het doel van de gegevensverwerking te bereiken, zorgt voor een onevenredige inbreuk op de privacy van betrokkenen.

De Raad voor de rechtspraak en de gerechten hebben, als (gezamenlijk) verwerkingsverantwoordelijken, kwaliteitsmanagement ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking in de zin van de AVG is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen.[10]

De AVG en de Wjsg bieden betrokkenen de mogelijkheid om invloed uit te oefenen op onjuiste verwerking van hun gegevens. Betrokkenen kunnen onder bepaalde voorwaarden informatie opvragen, om rectificatie verzoeken en, indien gegevens niet langer noodzakelijk zijn, om verwijdering verzoeken. Voor de uitoefening van deze rechten is een interne procedure opgesteld[11]. Daarnaast kunnen betrokkenen informatie vinden op rechtspraak.nl.[12]

[10] Overweging 39 AVG en art. 5 lid 1 sub d AVG

[11] 5.1(2)h [redacted]

4.1 Juistheid en nauwkeurigheid

Nummer	Norm	Referentie
PN 03-01	De verwerkingsverantwoordelijke heeft de nodige maatregelen getroffen om de juistheid en nauwkeurigheid van persoonsgegevens te waarborgen.	Art. 5 lid 1d AVG Art. 3 lid 1 Wjsg
PN 03-02	De verwerkingsverantwoordelijke voert periodiek controles op de werking van de getroffen maatregelen en brengt hierover rapportages uit aan het hogere management.	Art. 24 lid 1 AVG
PN 03-03	De verwerkingsverantwoordelijke controleert, voor zover praktisch uitvoerbaar, de kwaliteit van de gegevens voordat de gegevens worden verstrekt. Voor zover mogelijk wordt bij de doorzending van de gegevens de noodzakelijke informatie toegevoegd aan de hand waarvan de ontvangende bevoegde autoriteit de mate van juistheid, volledigheid en betrouwbaarheid van de gegevens kan beoordelen, alsmede de mate waarin zij actueel zijn.	Art. 3 lid 5 Wjsg

4.2 Rechten van betrokkenen

4.2.1 Algemeen

Nummer	Norm	Referentie
PN 03-04	De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van een **verzoek** dat valt onder de AVG informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkings-verantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.	Art. 12 lid 3 AVG
PN 03-05	De verwerkingsverantwoordelijke stelt de betrokkene binnen vier weken schriftelijk in kennis met betrekking tot de opvolging van zijn verzoek indien het verzoek betrekking heeft op persoonsgegevens die verwerkt worden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.	Art. 22 lid 4 Wjsg
PN 03-06	De verwerkingsverantwoordelijke reageert schriftelijk of met andere middelen; indien passend met elektronische middelen. Als de betrokkene daarom verzoekt kan de informatie, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is, mondeling worden meegedeeld.	Art. 12 lid 1 en 3 AVG
PN 03-07	Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, deelt hij deze laatste onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek mee waarom het verzoek zonder gevolg is gebleven en informeert hij hem over de mogelijkheid om een klacht in te dienen bij de bevoegde toezichthouder en beroep bij de rechter in te stellen.	Art. 12 lid 4 AVG
PN 03-08	Een beslissing op een verzoek om inzage, rectificatie en aanvulling van gerechtelijke strafgegevens geldt als een beschikking in de zin van art. 1:3 lid 2 Awb.	Art. 51f lid1 jo. 23 lid 1 Wjsg
PN 03-09	De verwerkingsverantwoordelijke stelt iedere ontvanger, aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie, gegevenswissing of verwerkingsbeperking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.	Art. 19 AVG
PN 03-10	Als de verwerkingsverantwoordelijke kan aantonen dat hij de betrokkene niet kan identificeren of wanneer de verwerkingsverantwoordelijke redenen heeft om te twijfelen aan de persoon die het verzoek doet, stelt hij de betrokkenen daarvan zo mogelijk in kennis. Betrokkene kan aanvullende gegevens verstrekken om identificatie mogelijk te maken[13]. Tot die tijd kan betrokkene zijn rechten niet uitvoeren.	Art. 12 lid 6 AVG Overweging 57 AVG Art. 51f lid 2 jo. 20 wjsg
PN 03-11	Het verstrekken van de informatie en het verstrekken van de communicatie is kosteloos, tenzij de verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter en dit kan worden aangetoond, mag de verwerkingsverantwoordelijke ofwel: a) AVG: een redelijke vergoeding aanrekenen in het licht van de	Art. 12 lid 5 AVG Art. 51f lid 1 jo. 25 lid 2 Wjsg

[13] Art. 11 en 12 AVG; overweging 57 AVG

	administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan ofwel: b) AVG, Wjsg, Wpg: weigeren gevolg te geven aan het verzoek.	

4.2.2 Recht van inzage

Nummer	Norm	Referentie
PN 03-12	De betrokkene krijgt bij honorering van zijn verzoek uitsluitsel over het al dan niet verwerken van hem betreffende persoonsgegevens.	Art. 15 AVG
PN 03-13	De inzage over de verwerkte persoonsgegevens bevat de volgende informatie: a) De verwerkingsdoeleinden; b) De betrokken categorieën persoonsgegevens; c) De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties; d) Indien mogelijk: de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen of, als dat niet mogelijk is, de criteria om die termijn te bepalen; e) Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat zijn persoonsgegevens te rectificeren of te wissen of de verwerking van de hem betreffende persoonsgegevens te beperken, alsmede het recht tegen die verwerking bezwaar te maken; f) Dat de betrokkene het recht heeft klacht in te dienen bij de bevoegde toezichthouder; g) Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschik- bare informatie over de bron van die gegevens; h) Het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, inclusief nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene; i) Bij doorgifte aan een derde land of een internationale organisatie en op verzoek van betrokkene de informatie over van de passende waarborgen; j) Op verzoek van betrokkene een kopie van de persoonsgegevens die worden verwerkt.	Art. 15 AVG
PN 03-14	Op basis van onderstaande uitzonderingen kan een verzoek van betrokkene worden afgewezen: a) De nationale veiligheid; b) De landsverdediging; c) De openbare veiligheid; d) De voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; e) Andere belangrijke doelstellingen van algemeen belang van de EU of van een lidstaat, met name een belangrijk economisch of financieel belang van de EU of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid; f) De bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures; g) De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;	Art. 23 lid 2 AVG en art. 41 lid 1 UAVG

	h) Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten (a), tot en met (e) en punt (g) bedoelde gevallen; i) De bescherming van de betrokkene of van de rechten en vrijheden van anderen; j) De inning van civielrechtelijke vorderingen.	
PN 03-15	De inzage doet geen afbreuk aan de rechten en vrijheden van anderen. Dit betekent dat bij honorering van een verzoek persoonsgegevens anderen onleesbaar gemaakt	Art. 14 lid 4 AVG
PN 03-16	De inzage van persoonsgegevens die vallen onder de werking van de Wjsg omvat, behoudens de onder PN 03-17 opgenomen weigeringsgronden en uitzonderingsgronden, de volgende informatie: a) De doeleinden van de verwerking; b) De rechtsgronden van de verwerking; c) De betrokken categorieën van persoonsgegevens; d) De vraag of de deze persoon betreffende persoonsgegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en over de ontvangers of categorieën van ontvangers aan wie de gegevens zijn verstrekt, met name ontvangers in derde landen of internationale organisaties; e) De voorziene bewaartermijn of, indien dat niet mogelijk is, de criteria om die termijn te bepalen; f) Het recht te verzoeken om rectificatie, vernietiging of afscherming van de verwerking van hem betreffende persoonsgegevens; g) Het recht een klacht in te dienen bij de bevoegde toezichthouder en de contactgegevens van die toezichthouder; h) De herkomst, voor zover beschikbaar, van de verwerking van de hem betreffende persoonsgegevens.	Art. 51f lid 1 jo. 18 Wjsg
PN 03-17	Een inzageverzoek op grond van de Wjsg wordt afgewezen voor zover dit een noodzakelijke en evenredige maatregel is: a) Ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures; b) Ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen; c) Ter bescherming van de openbare veiligheid; d) Ter bescherming van de rechten en vrijheden van derden; e) Ter bescherming van de nationale veiligheid; f) In geval van een kennelijk ongegrond of buitensporig verzoek, als bedoeld in artikel 25 lid 2 Wjsg.	Art. 51f lid 1 jo. 21 Wjsg
PN 03-18	Ten aanzien van minderjarigen die de leeftijd van zestien jaren nog niet hebben bereikt en ten aanzien van onder curatele gestelden, wordt een inzageverzoek gedaan door hun wettelijk vertegenwoordigers. De betrokken mededeling geschiedt eveneens aan de wettelijk vertegenwoordigers.	Art. 51f lid 1 jo. 20 lid 2 Wjsg
PN 03-19	Inzageverzoeken en rectificatieverzoeken in het kader van de Wjsg kunnen tevens worden gedaan door een advocaat aan wie de betrokkene een bijzondere machtiging heeft verleend met het oog op de uitoefening van zijn rechten krachtens deze wet en	Art. 51f lid 1 jo. 20 lid 4 Wjsg

	die het verzoek uitsluitend doet met de bedoeling de belangen van zijn cliënt te behartigen. De betrokken mededeling geschiedt aan de advocaat.	
PN 03-20	De communicatie vindt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is, plaats in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. Hierbij kan gebruik gemaakt worden van gestandaardiseerde iconen om het overzicht te houden.	Art. 12 lid 1 en lid 7 AVG Art. 51f lid 1 jo. 17b Wjsg
PN 03-21	De verwerkingsverantwoordelijke verstrekt gerechtelijke strafgegevens ten behoeve van de behandeling van strafzaken, in overeenstemming met het bepaalde bij of krachtens het Wetboek van Strafvordering.	Art. 51g lid 2 Wjsg

4.2.3 Recht op rectificatie

Nummer	Norm	Referentie
PN 03-22	Op verzoek van betrokkene worden onjuiste persoonsgegevens **gerectificeerd**.	Art. 16 lid 1 AVG Art. 22 lid 2 AVG
PN 03-23	Het **verzoek tot rectificatie** dient de aan te brengen wijzigingen te bevatten.	Art. 51f lid 1 jo. 22 lid 1 Wjsg
PN 03-24	Op verzoek van betrokkene worden onvolledige persoonsgegevens **vervolledigd of aangevuld** (met inachtneming van de doeleinden van de verwerking), onder meer op basis van een aanvullende verklaring van betrokkene.	Art. 16 lid 1 AVG Art. 51f lid 1 jo. 22 lid 1 Wjsg
PN 03-25	De verwerkingsverantwoordelijke geeft de **rectificatie** van de gerechtelijke strafgegevens door aan de bevoegde autoriteit van wie de gegevens afkomstig zijn en aan de ontvangers aan wie hij gerechtelijke strafgegevens heeft verstrekt.	Art. 51f lid 1 jo. 24 lid 1 Wjsg
PN 03-26	Indien de betrokkene verzoekt om **rectificatie** wordt hij schriftelijk in kennis gesteld van de ontvangst van het verzoek, de termijn voor uitsluitsel, de gehele of gedeeltelijke afwijzing van het verzoek en de mogelijkheid om naar aanleiding daarvan een klacht in te dienen bij de toezichthouder en beroep bij de rechter in te stellen.	Art. 51f lid 1 jo. 21 lid 1 Wjsg
PN 03-27	Een verzoek om **rectificatie** wordt afgewezen voor zover dit een noodzakelijke en evenredige maatregel is: a) Ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures; b) Ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen; c) Ter bescherming van de openbare veiligheid; d) Ter bescherming van de rechten en vrijheden van derden; e) Ter bescherming van de nationale veiligheid; In geval van een kennelijk ongegrond of buitensporig verzoek, als bedoeld in artikel 24 a lid 4 Wpg respectievelijk artikel 25 lid 2 Wjsg.	Art. 51f lid 1 jo. 21 lid 2 Wjsg

4.2.4 Recht op gegevenswissing

Nummer	Norm	Referentie
PN 03-28	Op verzoek van de betrokkene worden de hem betreffende persoonsgegevens **gewist** wanneer een van de volgende gevallen van toepassing is: a) De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt; b) De betrokkene trekt de toestemming waarop de verwerking berust in en er is geen andere rechtsgrond voor de verwerking; c) De betrokkene maakt bezwaar tegen de verwerking en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking. d) De persoonsgegevens zijn onrechtmatig verwerkt; e) De persoonsgegevens moeten worden gewist om te voldoen aan een in het wettelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust; f) De persoonsgegevens van kinderen jonger dan 16 jaar zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.	Art. 17 lid 1 AVG
PN 03-29	Op schriftelijk verzoek van de betrokkene worden de hem betreffende gerechtelijke strafgegevens, zonder onnodige vertraging **vernietigd**; 1. Indien de gegevens in strijd met een wettelijk voorschrift worden verwerkt, of 2. Om te voldoen aan een wettelijke verplichting.	Art. 51f lid 1 jo. 22 lid 2 Wjsg
PN 03-30	Wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en verplicht is de persoonsgegevens te **wissen**, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen om verwerkingsverantwoordelijken die de persoonsgegevens verwerken ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar of kopie of reproductie van, die persoonsgegevens te wissen.	Art. 17 lid 2 AVG
PN 03-31	Indien Onze Minister heeft vastgesteld dat onjuiste justitiële gegevens zijn verstrekt, of dat de justitiële gegevens onrechtmatig zijn verstrekt stelt hij de ontvangers onverwijld hiervan in kennis. In dat geval dienen de gegevens te worden gerectificeerd, vernietigd of te worden afgeschermd.	Art. 51f lid 1 jo. 24 Wjsg

4.2.5 Recht op beperking van de verwerking

Nummer	Norm	Referentie
PN 03-32	Op verzoek van betrokkene wordt de verwerking tijdelijk gestopt (**beperkt)**, indien: a) De juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoons- gegevens te controleren; b) De verwerking onrechtmatig en de betrokkene zich verzet tegen het wissen van de persoons- gegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan; c) De verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene deze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of: d) De betrokkene bezwaar heeft gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.	Art. 18 lid 1 AVG
PN 03-33	Wanneer de verwerking op grond van PN 03-26 is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.	Art. 18 lid 2 AVG
PN 03-34	In plaats van vernietiging draagt de verwerkingsverantwoordelijke zorg voor afscherming als: 1. De juistheid van de gegevens door de betrokkene wordt betwist en de juistheid, of onjuistheid niet kan worden geverifieerd, in welk geval de verwerkingsverantwoordelijke de betrokkene informeert voordat de afscherming wordt opgeheven, of 2. De gegevens moeten worden bewaard als bewijsmateriaal	Art. 51f lid 1 jo. 22 lid 3 Wjsg

4.2.6 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Nummer	Norm	Referentie
PN 03-35	De betrokkene heeft het recht de hem betreffende persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke **over te dragen** zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt, als de verwerking berust op: a) Toestemming van betrokkene, of: b) Een overeenkomst waarbij de betrokkene partij is of de verwerking via geautomatiseerde procedés wordt verricht; en geldt niet als: a) De verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend; b) Het afbreuk doet aan de rechten en vrijheden van anderen. Niet van toepassing onder de Wjsg	Art. 20 lid 1 AVG Art. 20 lid 3 AVG
PN 03-36	De betrokkene kan de gegevens rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere laten **overdragen** indien PN 03-33 geldt en dit technisch mogelijk is. Niet van toepassing onder de Wjsg	Art. 20 lid 2 AVG

4.2.7 Recht van bezwaar

Nummer	Norm	Referentie
PN 03-37	Betrokkene heeft het **recht om bezwaar** te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van een taak van algemeen belang[14] of een gerechtvaardigd belang[15]. Bij bezwaar van betrokkene wordt de verwerking gestaakt, tenzij er dwingende gerechtvaardigde gronden voor de verwerking kunnen worden aangevoerd die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering. Onder de Wjsg is in het geheel geen recht van bezwaar, zoals in de AVG aan de orde. De betrokkene heeft wel het recht om zich tot de toezichthouder te wenden om een klacht in te dienen, te bemiddelen of te adviseren.	Art. 21 lid 1 AVG Art 51f, lid 1 jo. 23 lid 2 Wjsg. Zie verder ook: art. 51h, lid 1 jo. 26a Wjsg.

[14] Art. 6 lid 1 onder e AVG
[15] Art. 6 lid 1 onder f AVG

5 Management van privacyrisico’s

Risicomanagement ondersteunt het gehele proces van signaleren tot wegwerken van de gesignaleerde risico’s door het nemen van maatregelen. Deze maatregelen moeten gebaseerd zijn op een risicoanalyse en wettelijke verplichtingen. Managen van risico’s is als een cyclisch proces ingericht.

Risicomanagement wordt binnen de Rechtspraak aantoonbaar toegepast op basis van de Minimumnorm Risicoanalyse IT (voor IT) en de Minimumnorm Risicobeheer (voor niet IT). Hiermee wordt het cyclische proces (op basis van PDCA) geborgd.

Het doel van risicomanagement is persoonsgegevens te beschermen tegen verlies, onbeschikbaarheid, corruptie en enige vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.

5.1 Managen van privacyrisico's

Nummer	Norm	Referentie
PN 04-01	Door de verwerkingsverantwoordelijke wordt voorafgaand aan de verwerking van persoonsgegevens een PIA uitgevoerd en goedgekeurd. [16] Uit de PIA blijken de passende maatregelen die moeten worden genomen. Een PIA kan meerdere doelen en (daaraan gerelateerde) verwerkingen omvatten.	Art. 35 AVG Art. 51f lid 1 jo. 7b Wjsg
PN 04-02	De verwerkingsverantwoordelijk wint voorafgaand aan de goedkeuring van een PIA het advies in van de Functionaris voor Gegevensbescherming. De verwerkingsverantwoordelijke volgt het advies op, tenzij er zwaarwegende redenen zijn om van het advies af te wijken. De afwijking wordt aan de Functionaris voor Gegevensbescherming medegedeeld en schriftelijk vastgelegd.	Art. 35 lid 2 AVG
PN 04-03	Van alle verwerkingen waarop een Dpia is uitgevoerd is een definitieve PIA rapportage bij de verwerkingsverantwoordelijke beschikbaar, waardoor bekend is welke risico's bestaan en welke maatregelen (moeten) worden genomen.	CIP B.03 /03.01
PN 04-04	Ten minste wanneer sprake is van een verandering in het risicoprofiel van de verwerking, verricht de verwerkingsverantwoordelijke een (her)toetsing. Hiermee wordt beoordeeld of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling (PIA) wordt uitgevoerd en om te beoordelen of er nieuwe risico's zijn die maatregelen behoeven.	Art. 35 lid 11 AVG Art. 51f lid 1 jo. 7b lid 3 Wjsg
PN 04-05	De toezichthoudende autoriteit wordt door de verwerkingsverantwoordelijke geraadpleegd over de voorgenomen verwerking van persoonsgegevens, die in een nieuw gegevensbestand zullen worden opgenomen, wanneer: a. de aard van de verwerking, in het bijzonder met gebruikmaking van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkene met zich meebrengt; b. uit een gegevensbeschermingseffectbeoordeling, bedoeld in artikel 35 AVG en art. 7b Wjsg, blijkt dat de verwerking een hoog risico zou opleveren als de verwerkingsverantwoordelijke geen maatregelen treft om het risico te beperken.	Art. 36 AVG
PN 04-06	De maatregelen uit de PIA zijn geïmplementeerd door bij het ontwerp de principes van gegevensbescherming te hanteren (privacy by design) en door het hanteren van standaardinstellingen op de minst inbreukmakende optie (privacy by default)	Art. 25 AVG
PN 04-07	Een procesbeschrijving is aanwezig voor het uitvoeren van Dpia's en voor het opvolgen van de uitkomsten. Hieruit blijkt hoe periodiek de risico's, afhankelijk van hoogte, worden gecontroleerd.	CIP B.03 /03.02
PN 04-08	Het Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) wordt standaard gebruikt voor het uitvoeren van DPIA's.	CIP B.03 /03.04
PN 04-09	Privacy by Design en de Dpia en maken onderdeel uit van de risicomanagementorganisatie van de Rechtspraak.	CIP B.03 /03.05

[16] In de AVG staat dat een PIA alleen moet worden uitgevoerd indien sprake is van een 'hoog risico'. Binnen de Rechtspraak hanteren we het principe dat voor iedere verwerking een PIA moet worden uitgevoerd. Hiermee wordt meteen voldaan aan de documentatieplicht.

6 Informatievestrekking aan betrokkenen

Wie persoonsgegevens verstrekt aan een organisatie heeft het recht te weten waarvoor, op welke wijze en door wie deze gegevens worden gebruikt. De organisatie heeft hiertoe een informatieplicht. Deze informatieplicht geldt ook wanneer persoonsgegevens van anderen worden ontvangen.

De verwerkingsverantwoordelijke moet daarom bij elke verzameling van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar stellen. Dit stelt betrokkene in staat zijn rechten uit te oefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking.

De grondslag toestemming is voor de Rechtspraak in het primaire proces vaak niet mogelijk, omdat betrokkenen geen vrije toestemming kunnen geven. In de bedrijfsvoering is toestemming sneller mogelijk.

Hiermee wordt voorkomen dat een organisatie niet transparant is en niet kan verantwoorden dat aan de beginselen van behoorlijke en transparante gegevensverwerking wordt voldaan.

In deze minimumnorm wordt onder andere ingegaan op de eisen aan de grondslag toestemming (PN 01-05)

6.1 Informatieverstrekking

Nummer	Norm	Referentie
PN 05-01	Indien toestemming van betrokkene (PN 01-05) als grondslag voor verwerking gebruikt wordt, dan wordt deze voorafgaand aan de verwerking, het doorgeven aan derden en het verder verwerken verkregen. Dit geldt voor persoonsgegevens die via betrokkenen of anderen wordt of is verkregen.	Art. 6 lid 1 AVG Art. 14 lid 3 AVG
PN 05-02	De toestemming moet door de betrokkene vrijelijk gegeven kunnen worden. Niet van toepassing op de Wjsg	Art. 7 lid 4 AVG
PN 05-03	Bij aanbieden van een dienst aan een kind en het kind is jonger dan 16 jaar, dan is de toestemming of machtiging tot toestemming verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt[17]. Niet van toepassing op de Wjsg	Art. 8 lid 1 AVG
PN 05-04	Het verzoek om toestemming wordt in een begrijpelijke en gemakkelijk toegankelijke vorm opgesteld, in duidelijke en eenvoudige taal zodanig dat precies duidelijk is waarvoor betrokkene toestemming geeft en zodanig dat een duidelijk onderscheid kan worden gemaakt van andere aangelegenheden waarvoor eventueel ook toestemming wordt gevraagd.	Art. 7 lid 2 AVG
PN 05-05	De verwerkingsverantwoordelijke verstrekt aan een betrokkene de in PN 05-08 en PN 05-09 bedoelde informatie over de verwerking van gerechtelijke strafgegevens in een beknopte en toegankelijke vorm. De informatie wordt met passende middelen, waaronder elektronische, verstrekt en in het algemeen in dezelfde vorm als het verzoek.	Art. 17b lid 1 Wjsg
PN 05-06	De informatie die aan betrokkene moet worden verstrekt, kan worden getoond op de website van de meest gerede partij	CIP U.05 /01.01b
PN 05-07	Wanneer persoonsgegevens bij de betrokkene worden verzameld, ontvangt de betrokkene de volgende informatie: a) De identiteit en contactgegevens van de verantwoordelijke en, in voorkomend geval, zijn of haar vertegenwoordiger; b) In voorkomend geval de contactgegevens van de Functionaris voor gegevensbescherming; c) De verwerkingsdoeleinden en ook de rechtsgrond van de gegevensverwerking; d) De gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde indien de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is[18]; e) In voorkomend geval de ontvangers of categorieën van ontvangers van persoonsgegevens; f) In voorkomend geval dat de verwerkingsverantwoordelijke het voornemen	Art. 13 AVG Art. 6 lid 1f AVG art. 18 lid 1 en art. 22 lid 1 en 2 Wjsg Art. 17a Wjsg

[17] Art. 8 AVG
[18] Art. 6 lid 1f AVG

	heeft de persoonsgegevens door te geven aan een derde land of internationale organisatie of een adequaatheidsbesluit van de commissie bestaat, welke de passende waarborgen zijn en hoe deze kunnen worden ingezien; g) De periode dat de gegevens worden opgeslagen of de criteria ter bepaling van die termijn; h) Dat de betrokkene recht heeft op inzage, rectificatie of wissing of beperking van de hem betreffende verwerking en het recht heeft bezwaar tegen de verwerking te maken en dat de betrokkene het recht heeft op gegevensoverdraagbaarheid; i) Dat de betrokkene zijn toestemming te allen tijde kan intrekken (voor zover de verwerking is gebaseerd op de rechtsgrond toestemming); j) Dat de betrokkene een klacht mag indienen bij de toezichthouder; k) Of de verstrekking een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten; l) Of de betrokkene verplicht is de gegevens te verstrekken en wat de mogelijke gevolgen zijn als deze de gegevens niet verstrekt; m) Of geautomatiseerde besluitvorming en/of profilering bestaat en in die gevallen nuttige informatie over de onderliggende logica alsmede het belang en de verwachte gevolgen voor de betrokkene; n) Informatie over het andere doel, wanneer een verwerking gaat plaatsvinden voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld.	
PN 05-08	De verwerkingsverantwoordelijke verstrekt de volgende informatie aan de betrokkene: a) de identiteit en contactgegevens van de verantwoordelijke en, in voorkomend geval, van de functionaris voor gegevensbescherming; b) de verwerkingsdoelen van gerechtelijk strafgegevens; c) het recht een klacht in te dienen bij de Autoriteit persoonsgegevens of de Procureur Generaal, en de contactgegevens van die autoriteit; d) de rechten van betrokkene, bedoeld in art. 18 lid 1 en art. 22 lid 1 en 2 Wjsg	
PN 05-09	In specifieke gevallen, om het voor betrokkene mogelijk te maken zijn rechten op grond van de Wjsg uit te oefenen, verstrekt de verwerkingsverantwoordelijke de volgende informatie aan de betrokkene: a) de rechtsgrondslag van de verwerking; b) de bewaartermijn van de gerechtelijke strafgegevens; c) in voorkomend geval, de categorieën van de ontvangers van de gerechtelijke strafgegevens; d) indien noodzakelijk, extra informatie, in het bijzonder wanneer de gerechtelijke strafgegevens zonder medeweten van de betrokkene worden verzameld; e) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 7e lid 1 Wjsg bedoelde profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.	Art. 17b Wjsg
PN 05-10	Wanneer persoonsgegevens bij een ander dan de betrokkene worden verzameld, ontvangt de betrokkene de volgende informatie: a) De identiteit en de contactgegevens van de verwerkingsverantwoordelijke en in voorkomend geval van de vertegenwoordiger van de	Art. 14 AVG

	verwerkingsverantwoordelijke; b) In voorkomend geval de contactgegevens van de Functionaris voor gegevensbescherming; c) De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking; d) De betrokken categorieën persoonsgegevens; e) In voorkomend geval de ontvangers of categorieën van ontvangers van de persoonsgegevens; f) Als persoonsgegevens aan een ontvanger in een derde land of aan een internationale organisatie wordt doorgegeven, wordt informatie gegeven over hoe een kopie kan worden verkregen over de waarborgen of voorschriften of waar ze kunnen worden geraadpleegd; g) De periode gedurende welke de persoonsgegevens zullen worden opgeslagen of indien dat niet mogelijk is de criteria om die termijn te bepalen; h) Indien van toepassing de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde; i) Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage, en rectificatie of wissing van persoonsgegevens of om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid; j) Wanneer verwerking is gebaseerd is op toestemming van betrokkene, heeft de betrokkene het recht de toestemming te allen tijde in te trekken. Dit doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming van vóór de intrekking; k) Dat de betrokkene het recht heeft een klacht in te dienen bij een AP; l) De bron waar de persoonsgegevens vandaan komen en in voorkomend geval of zij afkomstig zijn van openbare bronnen; m) Het bestaan van geautomatiseerde besluitvorming (inclusief profilering) inclusief de informatie over de onderliggende logica en het belang en de verwachte gevolgen van die verwerking voor de betrokkene.	

7 Bewaren van persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld en niet langer dan de bewaartermijn die sectorspecifieke wetgeving stelt. De bewaartermijn kan worden beëindigd door actieve verwijdering van gegevens of door anonimiseren van de persoonsgegevens. Bij anonimiseren zijn de gegevens niet meer herleidbaar tot de betrokkenen.[19]

Deze minimumnorm beoogt ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het te bereiken doel.[20] Hiermee kan worden voorkomen dat te lang bewaarde persoonsgegevens worden verwerkt voor andere dan de oorspronkelijke verwerkingsdoeleinden.

[19] Overweging 27 AVG
[20] Art. 5 lid 1e AVG

7.1 Bewaren van persoonsgegevens

Nummer	Norm	Referentie
PN 06-01	Van alle persoonsgegevens is de bewaartermijn vastgesteld en bekrachtigd. Deze bewaartermijn is de maximale periode waarin het noodzakelijk is dat de persoonsgegevens worden bewaard om het doel van de verwerking te bereiken.	Art. 5 lid 1e AVG
PN 06-02	Als in sectorspecifieke wetgeving een bewaartermijn is vastgelegd voor specifieke persoonsgegevens, dan gaat die bewaartermijn boven een bewaartermijn in PN 06-01	
PN 06-03	Binnen de Rechtspraak zijn kaders opgesteld die helpen bij het bepalen van de bewaartermijnen in PN 06-01. Hierin wordt onder ander gebruikgemaakt van de geldende Basisselectiedocumenten (BSD).	
PN 06-04	Wanneer persoonsgegevens voor langere periode dan noodzakelijk voor het te bereiken doel worden opgeslagen, dan is dit enkel toegestaan indien deze worden verwerkt met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, en zijn voor de rechten en vrijheden van de betrokkene ("opslagbeperking") passende waarborgen getroffen in overeenstemming met de AVG .	Art. 5 lid 1e AVG Art. 89 lid 1 AVG
PN 06-05	Als de bewaartermijnen verlopen, dienen de gegevens te worden verwijderd, vernietigd of geanonimiseerd.	Art. 5 lid 1e AVG jo. overweging 27 AVG. Art. 51g Wjsg

8 Doorgifte van persoonsgegevens

Doorgifte van persoonsgegevens kan plaatsvinden aan verwerker(s) en aan andere verwerkingsverantwoordelijke(n) buiten de EU/EER. Bij de doorgifte wordt onderscheid gemaakt tussen doorgifte binnen de EU/EER, waar de AVG geldt, en doorgifte naar partijen buiten de EU/EER. Als doorgifte naar partijen buiten de EU/EER plaatsvindt, dan spreekt de AVG van doorgifte aan derde landen en internationale organisaties.

Voor de Rechtspraak is tevens van belang dat de AVG en de Richtlijn niet van toepassing zijn voor partijen in Aruba, Curaçao en Sint Maarten. Hoewel Caribisch Nederland (ook wel bekend als de BES-eilanden: Bonaire, Sint Eustatius en Saba) onderdeel is van het land Nederland, zijn ook daar de AVG en de Richtlijn niet van toepassing. Voor Caribisch Nederland geldt wel de Wet bescherming persoonsgegevens BES en de Wet politiegegevens BES, maar er bestaat géén Wjsg BES.

Het doel van deze minimumnorm is waarborgen dat persoonsgegevens op een rechtmatige manier worden doorgegeven, op een juiste manier worden gebruikt en dat de verantwoordelijkheid voor deze rechtmatigheid en juistheid ingeregeld blijft. Hiermee wordt voorkomen dat persoonsgegevens onrechtmatig worden doorgegeven, onrechtmatig verder worden verwerkt en er een gebrek is aan het nemen van verantwoordelijkheid en controle.

8.1 Algemene regels bij doorgifte van persoonsgegevens

Nummer	Norm	Referentie
PN 07-01	Bij doorgifte van persoonsgegevens aan een andere verwerkingsverantwoordelijke zijn: a) De respectieve verantwoordelijkheden duidelijk, zodat zij aan hun AVG-verplichtingen voldoen, met name met betrekking tot: 1. De uitoefening van de rechten van de betrokkene, en; 2. Het informeren van de betrokkenen bij ontvangst b) de regeling met de respectieve verantwoordelijkheden aan de betrokkene beschikbaar gesteld.	Art. 26 lid 1 en lid 3 AVG
PN 07-02	De verwerking van persoonsgegevens door een verwerker[21] is in een schriftelijke overeenkomst of andere schriftelijke rechtshandeling vastgelegd, met daarin : a) Het onderwerp en de duur van de verwerking; b) De aard en het doel van de verwerking waarvoor de persoonsgegevens worden verstrekt, inclusief: a. Welke persoonsgegevens worden verstrekt aan de verwerker; b. Hoe dataminimalisatie is toegepast; c) Het soort persoonsgegevens, inclusief a. De classificatie van de persoonsgegevens; d) De categorieën van betrokkenen; e) De rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven; f) De persoonsgegevens uitsluitend verwerkt worden op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften; g) De gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden; h) De beveiliging van de verwerking is geborgd, inclusief: • Welke medewerkers van de verwerker toegang tot de persoonsgegevens nodig hebben; • Welke procedure wordt gevolgd in geval van een datalek; • In welke landen de persoonsgegevens worden opgeslagen; i) De vereisten aan de verwerkers gelden ook als vereisten voor het in dienst nemen van een andere verwerker. Daarnaast schakelt de verwerker geen andere verwerker in dan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van een algemene schriftelijke toestemming informeert de verwerker de verwerkingsverantwoordelijke over de toevoeging of vervanging van andere verwerkers, met de mogelijkheid van bezwaar door de verwerkingsverantwoordelijke. j) Passende technische en organisatorische maatregelen zijn genomen als betrokkene zijn rechten doet gelden, inclusief:	Art 28 lid 3 AVG Art. 28 lid 9 AVG Art. 51f lid 1 jo. 7d Wjsg Art. 1e Bjsg

[21] Art. 4 lid 8 AVG omschrijft een verwerker als: “een natuurlijke person of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwordelijke persoonsgegevens verwerkt”

	• Hoe de betrokkene wordt geïnformeerd over het uitbesteden van de persoonsgegevens aan de verwerker; • Het contact dat de verwerker mag hebben met de betrokkenen. k) De verwerkingsverantwoordelijke bijstand wordt verleend om te voldoen aan zijn verplichtingen ten aanzien van het borgen de van beveiliging van de verwerking; l) Na afloop van de verwerkingsdiensten, naar gelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens worden wist of deze aan hem terugbezorgd worden en bestaande kopieën worden verwijderd; m) De verwerker alle informatie aan de verwerkingsverantwoordelijke ter beschikking stelt en bijdraagt ten behoeve van audits en om aan te kunnen tonen dat hij aan zijn verplichtingen voldoet, waaronder inspecties; en n) De verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis stelt als naar zijn mening een instructie inbreuk oplevert op de AVG of op andere wet- en regelgeving inzake gegevensbescherming.	
PN 07-03	De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over het toepassen van passende technische en organisatorische maat- regelen bieden.	Art. 28 lid 1 AVG Art. 51f lid 1 jo. 7d Wjsg
PN 07-04	Wanneer de verwerking niet had mogen plaatsvinden, dan wordt door de verwerkingsverantwoordelijke de doorgifte beëindigd en de toezichthoudende autoriteit en de betrokkenen hierover geïnformeerd.	Art. 49 AVG
PN 07-05	Gerechtelijke strafgegevens kunnen slechts worden verstrekt ten behoeve van beleidsinformatie, wetenschappelijk onderzoek en statistiek nadat aan de betrokken onderzoeker daartoe schriftelijk toestemming is verleend door het bestuur of de gerechtsbesturen met inachtneming van het informatieprotocol van de Rechtspraak.	Art. 31 lid 2 Bjsg

8.2 Doorgifte van persoonsgegevens naar landen buiten de EU

Nummer	Norm	Referentie
PN 07-06	Als een verwerkingsverantwoordelijke of verwerker niet in de EU is gevestigd, dan is door de verwerkingsverantwoordelijke of de verwerker schriftelijk een vertegenwoordiger in de EU aangewezen, tenzij: 1. Sprake is van een incidentele verwerking die geen grootschalige verwerking van bijzondere categorieën persoonsgegevens betreft, of: 2. Bij de verwerking van persoonsgegevens die verband houden met strafrechtelijke veroor- delingen en strafbare feiten en waarbij de kans gering is dat zij een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. **3.** Het een verwerking door een overheidsinstantie of overheidsorgaan betreft.	Art. 27 AVG
PN 07-07	De verwerking vindt niet plaats als er een rechterlijke uitspraak of een besluit van een administratieve autoriteit is van een derde land op grond waarvan een verwerkingsverant- woordelijke of een verwerker persoonsgegevens moet doorgeven of verstrekken en waarbij dit niet erkend of afdwingbaar is gemaakt dat dit is gebaseerd op een internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtsbijstand tussen het verzoekende derde landen en de EU of een lidstaat.	Art. 48 AVG
PN 07-08	Bij een gebrek aan een adequaatheidsbesluit kunnen in de wet- en regelgeving of bepalingen om gewichtige redenen van openbaar belang grenzen worden gesteld aan de doorgifte van specifieke categorieën persoonsgegevens aan een derde land of een internationale organisatie.	Art. 49 lid 5 AVG
PN 07-09	Doorgifte van persoonsgegevens naar buiten de EU is alleen toegestaan, wanneer naar het oordeel van de Europese Commissie in het derde land, in het gebied of in één of meerdere nader bepaalde sectoren in het derde land of bij de internationale organisatie in kwestie een passend beschermingsniveau is gewaarborgd[22].	Art. 45 AVG Art. 51f lid 1 jo. 16 lid 1 Wjsg
PN 07-10	Wanneer met een land geen adequaatheidsbesluit is afgesloten, is doorgifte alsnog mogelijk indien passende waarborgen zijn getroffen. Van passende waarborgen is sprake wanneer er: a) Een juridisch bindend en afdwingbaar instrument tussen overheidsinstanties of –organen is afgesloten; b) Door de toezichthoudende autoriteit bindende bedrijfsvoorschriften zijn goedgekeurd (zie ook PN 07-12); c) Standaardbepalingen zijn inzake gegevensbescherming die in de door de Europese Commissie bedoelde onderzoeksprocedure zijn vastgesteld; d) Standaardbepalingen zijn inzake gegevensbescherming die door een toezichhoudende autoriteit zijn vastgesteld en die in de door de Europese Commissie bedoelde onderzoeksprocedure zijn goedgekeurd; e) Een goedgekeurde gedragscode is, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen toe te passen, waaronder waarborgen voor de rechten van de betrokkenen; f) Een goedgekeurd certificeringmechanisme is, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen, onder meer voor de	Art. 46 AVG Art. 93 lid 2 AVG

[22] Zogenaamde adequaatheidsbesluiten. Zie voor gepubliceerde besluiten de site van de Europese Commissie: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

	rechten van de betrokkenen, toe te passen, of: g) Door de bevoegde toezichthoudende autoriteit passende waarborgen zijn opgesteld, waarbij er met name: • contractbepalingen zijn tussen de verwerkingsverantwoordelijke of de verwerker en de verwerkingsverantwoordelijke, de verwerker of de ontvanger van de persoonsgegevens in het derde land of de internationale organisatie, of: • bepalingen zijn opgenomen in administratieve regelingen tussen overheidsinstanties of organen, waaronder afdwingbare en effectieve rechten van betrokkenen.	
PN 07-11	Wanneer door de Europese Commissie geen adequaatheidsbesluit is genomen, dan kunnen persoonsgegevens slechts worden verstrekt of doorgegeven, indien: a) In een juridisch bindend instrument passende waarborgen voor de bescherming van persoonsgegevens zijn geboden; of b) De verwerkersverantwoordelijke na beoordeling van alle omstandigheden heeft geconcludeerd dat het derde land of de internationale organisatie passende waarborgen biedt voor een zorgvuldige gegevensverwerking.	Art.51f lid 1 jo. 16a lid 2 Wjsg
PN 07-12	Als bindende bedrijfsvoorschriften (PN 07-10) worden gebruikt om passende waarborgen te bieden, dan: a) Zijn die juridisch bindend of van toepassing en worden deze gehandhaafd door alle betrokken leden van het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen; met inbegrip van hun werknemers; b) Dient aan betrokkenen uitdrukkelijk afdwingbare rechten te worden toegekend met betrekking tot de verwerking van hun persoonsgegevens, en: c) Worden hierin in ieder geval de volgende elementen vastgelegd (zie voor de volledige weergave art. 47 lid 2 AVG): 1. De structuur en de contactgegevens; 2. De gegevensdoorgiften of reeks van doorgiften; 3. Het intern en extern juridisch bindende karakter; 4. De toepassing van de algemene beginselen inzake gegevensbescherming; 5. De rechten van betrokkenen; 6. De aanvaarding van aansprakelijkheid voor alle inbreuken; 7. De wijze waarop informatie wordt verschaft over de bindende bedrijfsvoorschriften; 8. De taken van elke Functionaris voor gegevensbescherming, of elke andere persoon of entiteit die is belast met het toezicht op: • De naleving van de bindende bedrijfsvoorschriften binnen het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen, • Opleiding, en: • De behandeling van klachten; 9. De klachtenprocedures; 10. De bestaande procedures om te controleren of de bindende bedrijfsvoorschriften zijn nageleefd; 11. De procedures om die veranderingen in de regels te melden, te registreren en aan de toezichthouder te melden; 12. De procedure voor samenwerking met de toezichthouder;	Art. 47 AVG

	13. De procedures om eventuele wettelijke voorschriften aan de toezichthouder te melden, en: 14. De passende opleiding inzake gegevensbescherming voor personeel.	
PN 07-13	De doorgifte mag ook plaatsvinden als: a) De betrokkene uitdrukkelijk heeft ingestemd met de voorgestelde doorgifte, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen, tenzij dit door een overheidsinstantie ten behoeve van een openbare bevoegdheid wordt verricht; b) De doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen, tenzij dit door een overheidsinstanties ten behoeve van een openbare bevoegdheid wordt verricht; c) De doorgifte noodzakelijk is voor de sluiting of de uitvoering van een in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke persoon of rechtspersoon gesloten overeenkomst, tenzij dit door een overheidsinstanties ten behoeve van een openbare bevoegdheid wordt verricht; d) De doorgifte noodzakelijk is wegens gewichtige redenen van algemeen belang, dat is erkend bij de wet- en regelgeving; e) De doorgifte noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering; f) De doorgifte noodzakelijk is voor de bescherming van de vitale belangen van de betrokkene of van andere personen, als de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven; g) De doorgifte verricht is vanuit een register dat volgens het Wettelijk recht is bedoeld om het publiek voor te lichten en dat door eenieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen kan worden geraadpleegd, maar alleen voor zover in het geval in kwestie wordt voldaan aan de in het wettelijk recht vastgestelde voorwaarden voor raadpleging; h) De doorgifte aan derde landen of internationale organisaties is gebaseerd op internationale overeenkomsten die door de lidstaten zijn gesloten vóór 24 mei 2016 en die overeenkomsten in overeenstemming zijn met het vóór die datum toepasselijke Unierecht en nog niet is gewijzigd, vervangen of ingetrokken.	Art. 49 AVG Art. 96 AVG
PN 07-14	Bij ontbreken van een adequaatheidsbesluit of van passende waarborgen, is doorgifte van persoonsgegevens aan een derde land of internationale organisatie slechts toegelaten, indien de doorgifte noodzakelijk is: a) Om vitale belangen van de betrokkene of van een andere persoon te beschermen; b) Om de legitieme belangen van de betrokkene te beschermen wanneer het recht van de lidstaat van waaruit de doorgifte van persoonsgegevens plaatsvindt zulks bepaalt; c) Om een onmiddellijke en ernstige bedreiging van de openbare veiligheid van een lidstaat of een derde land te voorkomen; d) In afzonderlijke gevallen met het oog op de strafrechtspleging;	Art. 51f lid 1 jo. 16a lid 3 Wjsg

	e) In afzonderlijke gevallen met het oog op het instellen, uitoefenen of verdedigen van rechtsvorderingen met het oog op de strafrechtspleging; En de grondrechten en fundamentele vrijheden van de betrokkene zwaarder wegen dan het algemeen belang van de doorgifte bedoeld onder d) en e).	

9 Intern toezicht

De doelstelling van deze minimumnorm is te zorgen voor en/of vast te stellen dat maatregelen ter waarborging van de privacy afdoende zijn ingericht. Deze minimumnorm bevat de normen voor het intern toezicht op de rechtmatigheid van de gegevensverwerking. Een gegevensverwerking is rechtmatig als deze voldoet aan de eisen die de AVG, sectorspecifieke wetgeving en/of een (eventuele) Gedragscode stelt.

De toegang tot de gegevensverwerking voor betrokkene (het inzagerecht en de informatieplicht) worden genoemd in de Minimumnorm Privacy – Datakwaliteit en Rechten van betrokkene. Daarnaast bevat het Handboek Datalekken Gerechten de normen voor de afhandeling van datalekken.

9.1 Intern toezicht op de rechtmatigheid van gegevensverwerking

Nummer	Norm	Referentie
PN 08-01	De verwerkingsverantwoordelijke controleert of de gegevensverwerkingen voldoen aan de wettelijke verplichtingen. Hiertoe worden door de verwerkingsverantwoordelijke periodiek compliancy assessments op in ieder geval de onderstaande normen uitgevoerd en de resultaten geregistreerd. De verwerkingsverantwoordelijke deelt de informatie met de Functionaris voor gegevensbescherming, zodat deze toezicht kan houden.	Art. 5 lid 2 AVG
PN 08-02	Als blijkt dat toch niet voldaan wordt aan de eisen van de AVG, dan rapporteert de verwerkingsverantwoordelijke over de te nemen maatregelen om de privacyschending te beëindigen. De evaluatierapportages worden beschikbaar gesteld aan Functionaris voor gegevensbescherming.	Art. 5 lid 2 AVG
PN 08-03	Per jaar wordt op basis van onderstaande normen door de gerechtsbesturen c.q. de directies van de landelijke diensten aan de Functionaris voor gegevensbescherming een planning van activiteiten opgeleverd, zodat helder is in hoeverre voldaan wordt aan de privacywetgeving.	Art. 5 lid 2 AVG
PN 08-04	De verwerkersverantwoordelijke toont aan dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt (doelbinding).	Art. 5 lid 1 sub b en 2 AVG Art. 51f lid 1 jo. 3 lid 3 en 6 Wjsg
PN 08-05	De verwerkingsverantwoordelijke toont aan dat de verwerking toereikend is, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking).	Art. 5 lid 1 sub c en lid 2 AVG Art. 3 lid 3 Wjsg
PN 08-06	De verwerkingsverantwoordelijke toont aan dat de verwerking ten aanzien van de betrokkene rechtmatig is.	Art. 5 lid 1 sub a en lid 2 AVG Art. 51f lid 1 jo. 3 lid 3 Wjsg
PN 08-08	De verwerkingsverantwoordelijke toont passende technische en organisatorische maatregelen op een dusdanige manier worden verwerkt, dat een passende beveiliging ervan gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwelijkheid).	Art. 5 lid 1 sub f en lid 2 AVG Art. 51f lid 1 jo. 3 lid 4 Wjsg
PN 08-09	De verwerkingsverantwoordelijke toont aan dat de persoonsgegevens juist zijn en zo nodig worden geactualiseerd en waarbij alle redelijke maatregelen moeten zijn genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.	Art. 5 lid 1 sub d en lid 2 AVG Art. 51f lid 1 jo. 3 lid 1 en 5 Wjsg
PN 08-10	De verwerkingsverantwoordelijke toont aan dat persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.	Art. 5 lid 1 sub e en 2 AVG Art. 51f lid 1 jo. 3 lid 7 Wjsg
PN 08-11	De verwerkingsverantwoordelijke toont aan dat de wijze van verwerken ten aanzien van de betrokkene behoorlijk is.	Art. 5 lid 1 sub a en lid 2 AVG Art. 51f lid 1 jo. 3 lid 3 Wjsg

PN 08-12	De verwerkingsverantwoordelijke toont aan dat de persoonsgegevens op een wijze worden verwerkt die voor de betrokkene transparant is.	Art. 5 lid 1 sub a en lid 2 VG
PN 08-13	De verwerkingsverantwoordelijke toont door middel van een (opgebouwd) dossier aan dat voldaan wordt aan de privacywetgeving.	Art. 5 lid 2 AVG
PN 08-14	Bij het aantonen van het compliant en het compleet zijn van het dossier wordt gebruikgemaakt van het register van verwerkingsactiviteiten.	Art. 30 AVG Art. 51f lid 1 jo. 26c Wjsg

Deelbesluit 1 - Datalekken
Document 17

de Rechtspraak

Contactpersoon
[redacted]
Adviseur integrale veiligheid en beveiliging
Rechtbank Overijssel
M 06 [redacted]
E [redacted]@rechtspraak.nl

Datum
20 april 2022

Bijlagen
1: Overzicht inc denten 10 februari 2020-25 januari 2022
2: Verstrekkingen aan verkeerde geadresseerde WZD, WvGGZ en Jeugd v3.pdf

Notitie

Aan	LOBRO
Van	[redacted] & [redacted]
Datum	20 april 2022
Onderwerp	Not tie datalekken digitale postkamer

Inleiding

De digitale postkamer is een systeem waarmee de administraties van de rechtbanken brieven, uitnodigingen en uitspraken aan partijen kunnen verstrekken. Eind 2021 is door IVO Rechtspraak bij het bureau BVA van de Raad voor de rechtspraak een melding gedaan dat een groot aantal datalekken is geconstateerd die ontstaan zijn bij het gebruik van de digitale postkamer. Deze bevindingen zijn in het LOBRO besproken, waarbij is afgesproken dat alle BVC's lokaal navraag zouden doen of de aantallen datalekken herkend werden bij de gerechten. Uit deze inventarisatie is naar voren gekomen dat geen enkel gerecht dit aantal datalekken herkende. Op basis van deze uitkomst is in het LOBRO besloten dat door twee BVC's nader onderzoek zou worden ingesteld. Dit onderzoek is afgerond en de uitkomsten daarvan zijn in dit memo beschreven.

Wat is de omvang van de geconstateerde datalekken in de digitale postkamer?

Uit de overzichten van IVO blijkt dat er in de periode 10 februari 2020 tot 25 januari 2022 3153 incidenten zijn geweest die kunnen worden aangeduid als mogelijk datalek. In bijlage 1 is een gedetailleerd overzicht van de incidenten bijgevoegd.

Alle incidenten zijn adresseringsfouten waarbij stukken mogelijk naar een verkeerde ketenpartner zijn verzonden. Deze adresseringsfouten zijn in twee categorieën onder te verdelen:

- Het zaaknummer dat wordt ingevoerd komt niet overeen met een bestaande indiening. Hierdoor wordt er geen koppeling gemaakt met de externe referentie van de ketenpartner en komt het bericht niet op de juiste wijze aan. Het gaat hier om de kolommen 1 en 2 (geen referentie).
- Een bericht met een bepaalde referentie is aan een verkeerde ketenpartner gestuurd. Het gaat hier om de kolommen 3 tot en met 8. Hierbij wordt bijvoorbeeld een bericht met een referentienummer van het OM naar het CIZ gestuurd. Op basis van het referentienummer is te zien dat dit de verkeerde ketenpartner is.

N.B. Het OM heeft haar IT zodanig ingericht dat berichten zonder referentie of met een onjuiste referentie in een uitvalbak worden geplaatst. Deze uitvalbak wordt iedere twee dagen zonder inzage geschoond.

Is er sprake van een datalek?

De AVG kent het begrip datalek niet, maar spreekt van een inbreuk in verband met persoonsgegevens. Hiervan is onder meer sprake als persoonsgegevens per ongeluk of op onrechtmatige wijze ongeoorloofd worden verstrekt. Kort samengevat, indien gegevens naar een verkeerde partij worden gestuurd, is sprake van een datalek. Een datalek moet worden gemeld aan de toezichthouder, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de privacy van betrokkenen. Een datalek moet ook aan de betrokkene worden gemeld als het datalek een hoog risico voor de betrokkene meebrengt. De incidenten die zijn ontstaan in de digitale postkamer zullen dus in veel gevallen een datalek vormen.

Moeten de datalekken gemeld worden bij de toezichthouder (PG Hoge Raad) of betrokkenen?

In deze situatie is sprake van verzending aan een professionele partij. Het risico voor betrokkenen is hierdoor verwaarloosbaar. Er is geen sprake van een hoog risico voor de rechten en vrijheden van betrokkenen waardoor kan worden afgezien van het melden aan de toezichthouder of betrokkene(n).

Gezien het aantal ontstane datalekken is het advies van het LOBRO aan de besturen om het risico te accepteren en de datalekken enkel te registreren in Classbase. Wel is het advies om voor nieuwe datalekken per individueel geval te beoordelen of het een meldenswaardig datalek is.

Hoe hebben deze datalekken kunnen ontstaan?

Bij de invoering van de digitale postkamer werd het systeem gebruikt voor de verstrekking van stukken aan slechts één ketenpartner. In deze situatie was het niet mogelijk om adresseringsfouten te veroorzaken. Bij uitbreiding van het gebruik van de digitale postkamer, waarbij meerdere ketenpartners op het systeem zijn aangesloten, zijn geen aanvullende privacy maatregelen getroffen om adresseringsfouten te voorkomen.

Wat is de huidige situatie?

Op dit moment zijn er door IVO een aantal technische maatregelen genomen om het aantal datalekken terug te dringen. Zo wordt de gebruiker er sinds 23 juni 2021 op geattendeerd wanneer een zaaknummer niet wordt gevonden. Dat gebeurt door middel van een waarschuwingsmelding die het systeem geeft. De inhoud van de melding is: "Bij dit zaaknummer is geen indiening gevonden. Hierdoor komt dit bericht NIET aan bij de ketenpartner". Daarnaast is op 7 februari 2022 is nog een controle ingevoerd, er wordt een waarschuwing getoond dat de zaaksoorten niet overeen komen van indiening en verstrekking: "Let op: deze zaak is ingediend met zaaksoort<indiening-zaaksoort>. Controleer de geselecteerde zaaksoort." Ook is eind december 2021 de knop 'Reageer op deze indiening' beschikbaar in de digitale postkamer, gegevens van de indiening worden dan automatisch overgenomen in de verstrekking (ketenpartner en zaaksoort).

Na de implementatie van deze maatregelen zien we dat het aantal incidenten ver is teruggelopen en het nog maar om enkele mogelijke datalekken per maand gaat (zie het overzicht in bijlage 2 voor de trend die zichtbaar is). Uit navraag bij de gebruikers blijkt dat deze datalekken veelal veroorzaakt worden door nieuwe medewerkers die de waarschuwingsmeldingen negeren en stukken toch versturen.

Hoe voorkomen we deze datalekken in de toekomst en hoe zorgen we ervoor dat datalekmeldingen van de digitale postkamer op de juiste manier worden opgepakt?

Met de invoering van de maatregelen die hierboven beschreven staan is het aantal datalekken tot een minimum teruggebracht en is het risico op dit moment laag. Hierdoor lijkt het op dit moment niet nodig aanvullende technische maatregelen te treffen.

Wel blijft het van belang datalekken die worden veroorzaakt in de digitale postkamer te blijven monitoren en beperken. Hiervoor worden de volgende adviezen gegeven:

1. Het onderwerp wordt besproken met de betreffende teamvoorzitter(s) waarbij wordt gevraagd om aandacht te hebben voor het onderwerp datalekken bij het inwerktraject voor nieuwe medewerkers, zodat waarschuwingen uit het systeem niet zonder geldige reden worden genegeerd.
2. De meldingen van incidenten die door IVO dagelijks worden verstuurd aan de functionele mailboxen van de betreffende afdelingen/teams worden ook verzonden naar de datalekmailboxen van de gerechten. Op deze manier wordt de privacy coördinator van ieder gerecht direct geïnformeerd en kan samen met het team/de afdeling de afweging worden gemaakt of het een meldenswaardig datalek betreft.
3. Al deze incidenten worden gemeld in Classbase ongeacht of het datalek wordt gemeld aan betrokkene of de toezichthouder. Het is de bedoeling dat alle gerechten deze meldingen op eenduidige wijze in Classbase registreren.

de Rechtspraak

Bijlage 1: Overzicht incidenten 10 februari 2020-25 januari 2022

Rijlabels	1. Geen referentie aan CIZ	2. Geen referentie aan OM	3. Verkeerd geadresseerd aan CIZ	4. Verkeerd geadresseerd aan CORV	5. Verkeerd geadresseerd aan OM met referentie	6. Wzd onterecht aan IGJ gestuurd	7. Wzd onterecht aan IGJ+	8. Corv onterecht aan IGJ gestuurd	Eindtotaal
Amsterdam	**20**	**103**	**12**		**29**	**30**	**211**		**405**
Amsterdam	20	103	12		29	30	211		405
Den Haag	**96**	**510**	**5**		**21**	**18**	**31**		**681**
's-Gravenhage	96	510	5		21	18	31		681
Gelderland	**74**	**148**	**7**	**4**	**19**	**16**	**62**	**2**	**332**
Arnhem	22	51	5	2	13	12	27		132
Zutphen	52	97	2	2	6	4	35	2	200
Limburg	**75**	**162**	**6**		**10**	**3**		**1**	**257**
Maastricht	27	35	2		7	3		1	75
Roermond	48	127	4		3				182
Midden-Nederland	**46**	**152**	**1**		**29**	**21**	**18**	**1**	**268**
Lelystad	32	12			1	1	3		49
Utrecht	14	140	1		28	20	15	1	219
Noord-Holland	**59**	**116**	**2**	**3**	**8**	**8**	**56**		**252**
Alkmaar	20	39			7	7	28		101
Haarlem	39	77	2	3	1	1	28		151
Noord-Nederland	**63**	**90**	**8**		**19**	**13**	**46**		**239**
Assen	31	27			3	3	2		66
Groningen	17	31	5		14	4	28		99
Leeuwarden	15	32	3		2	6	16		74
Oost-Brabant	**7**	**37**	**3**		**7**	**6**	**40**		**100**
's-Hertogenbosch	7	37	3		7	6	40		100
Overijssel	**5**	**38**	**2**	**1**	**10**	**8**	**4**		**68**
Almelo	5	15	1		5	5	1		32
Zwolle		23	1	1	5	3	3		36
Rotterdam	**27**	**178**	**2**		**23**	**19**	**92**	**2**	**343**
Dordrecht	11	41			7	7	30		96
Rotterdam	16	137	2		16	12	62	2	247
Zeeland-West-Brabant	**78**	**77**	**3**		**15**	**16**	**19**		**208**
Breda	71	62	1		13	14	14		175
Middelburg	7	15	2		2	2	5		33
Eindtotaal	**550**	**1611**	**51**	**8**	**190**	**158**	**579**	**6**	**3153**

Deelbesluit 1 - Datalekken
Document 18

Jaarrapportage

Integrale veiligheid en beveiliging

[redacted] januari 2019

Hoe sterk zijn de schakels van de Rechtspraak?

Ceci n'est pas une Powerpoint

Incidentenregistratie

de Rechtspraak

	2016	2017	2018
Veiligheid	141	134	191
Agressie en geweld	houdt geen verband met woo-verzoek		
(incidenten) Bij zittingen buiten gerechtsgebouw			
(poging tot) Suïcide			
(poging tot) Uitbraak			
(terroristische) Aanslag			
Dreigbrief			
Email of social media (agressie)			
Fysiek met wapens			
Fysiek zonder wapens (handgemeen)			
Gijzeling			
Gooien met voorwerpen			
Mondeling/telefonisch (agressie)			
Vandalisme			
Vernieling			
Bedrijfshulpverlening			
Besmettelijke ziekten			
Brand			
Bommelding			
Brandmelder (geactiveerd)			
Diverse			
Algehele spanningsuitval			
Diefstal			
Gas- en waterlekkage			
Schade door natuurverschijnselen			
Verdachte poststukken			

	2016	2017	2018
BEVEILIGING	126	150	148
Rijkspas	houdt geen verband met woo-verzoek		
Verlies doopkaarten			
Verloren rijkspassen			
Toegangscontrole			
Aanwezigheid pepperspray			
Aanwezigheid overige ongewenste goederen			
Aanwezigheid slag- en stootwapens			
Aanwezigheid steekwapens			
Aanwezigheid verboden geestbeïnvloedende middelen			
Aanwezigheid vuurwapens en/of munitie			
Overtreding minimumnorm toegangsverlening			
Vuurwerk aanwezig			
Overtreding huisregels			
Inbraak (alarm)			
Onrechtmatig gebruik audiovisuele middelen			
Ordeverstoring			
Overtreding minimumnorm persrichtlijn			
Verlies van fysieke sleutels			

	2016	2017	2018
INFORMATIEBEVEILIGING	64	110	419
Datalek - gemeld AP	0	29	196
Incident met REP-certificaat	0	0	0
Misbruik autorisaties	5	2	3
Overtreding minimumnorm email- en internetgebruik	6	2	1
Overtreding minimumnorm Rubricering	2	0	1
Verlies gegevens (papier en digitaal)	45	65	213
IT-security			
Centrale ICT-uitval	5.1(2)h		
(poging tot) Hacking			
Lokale ICT-uitval			
Malware-besmetting			
Phishing			
Social engineering			

Deelbesluit 1 - Datalekken
Document 19

Jaarrapportage

Integrale veiligheid en beveiliging

[redacted] januari 2020

Hoe sterk zijn de schakels van de Rechtspraak?

Ceci n'est pas une Powerpoint

1. In orde

Privacy

- Het handboek *Handboek datalekken* is binnen de gerechten grotendeels geïmplementeerd.
- De procedures om betrokkenen in staat te stellen hun privacyrechten uit te voeren werken bij alle gerechten.
- Met het borgingsplan privacy heeft de Rechtspraak een continu bijgewerkt overzicht van de benodige privacyverbeteringen.
- Het key control dashboard is uitgebreid met een AVG- privacymodule.

AVG proof

Incidentenregistratie

de Rechtspraak

	2017	2018	2019
Veiligheid	134	191	181
Agressie en geweld			
(incidenten) Bij zittingen buiten gerechtsgebouw	houdt geen verband met woo-verzoek		
(poging tot) Suïcide in cellengebied			
(poging tot) Uitbraak cellengebied			
(terroristische) Aanslag op de rechtspraak			
Dreigbrief			
Email of social media (agressie)			
Fysiek met wapens			
Fysiek zonder wapens (handgemeen)			
Gijzeling			
Gooien met voorwerpen			
Mondeling/telefonisch (agressie)			
Vandalisme			
Vernieling			
Bedrijfshulpverlening			
Besmettelijke ziekten			
Brand			
Bommelding			
Brandmelder (geactiveerd)			
Diverse			
Algehele spanningsuitval			
Diefstal binnen de gerechten			
Gas- en waterlekkage			
Schade door natuurverschijnselen (storm)			
Verdachte poststukken			

	2017	2018	2019
BEVEILIGING	150	148	180
Rijkspas	houdt geen verband met woo-verzoek		
Verlies doopkaarten			
Verloren rijkspassen			
Toegangscontrole			
Aanwezigheid pepperspray			
Aanwezigheid overige ongewenste goederen			
Aanwezigheid slag- en stootwapens			
Aanwezigheid steekwapens			
Aanwezigheid verboden geestbeïnvloedende middelen			
Aanwezigheid vuurwapens en/of munitie			
Overtreding minimumnorm toegangsverlening			
Vuurwerk aanwezig			
Overtreding (huis)regels			
Inbraak (alarm)			
Onrechtmatig gebruik audiovisuele middelen			
Ordeverstoring			
Overtreding minimumnorm persrichtlijn			
Verlies van fysieke sleutels			
Integriteitsschending (nieuw)			

	2017	2018	2019
INFORMATIEBEVEILIGING	110	419	583
Datalek - gemeld AP	29	196	95
Datalek – gemeld PG-HR (Nieuw)	-	-	75
Misbruik autorisaties	2	3	0
Overtreding minimumnorm email- en internetgebruik	2	1	0
Verlies gegevens (papier en digitaal)	65	213	398
IT-security			
Centrale ICT-uitval (langdurig)	5.1(2)h		
(poging tot) Hacking			
Lokale ICT-uitval			
Overtreding minimumnorm Rubricering			
Malware-besmetting			
(poging tot) Phishing			
Social engineering			
Externe meldingen a.g.v. Responsible Disclosure			

Verder opvallend in de incidentregistratie

Het jaar 2019 kenmerkt zich door:

houdt geen verband met woo-verzoek

- Een hoog aantal Datalekken en verlies van ander soort gegevens
- **Onachtzaamheid van medewerkers speelt momenteel de grootste rol bij het verlies van gegevens, zo blijkt uit de collegiale toets.**
  - Hierbij moet worden gedacht aan informatie opbergen in het verkeerde dossier en het versturen van informatie naar het verkeerde adres.
    - **Afgaande op de incidentenregistratie scoort het gerechtshof Amsterdam het best met 0 Datalekken, ook goed scoren de CRvB en het gerecht Noord-Holland met beide 1 Datalek.**

Deelbesluit 1 - Datalekken
Document 20

Jaarverslag Integrale beveiliging 2020

[redacted], februari 2021

Hoe sterk zijn de schakels van de Rechtspraak?

Ceci n'est pas une Powerpoint

1. In orde

Informatiebeveiliging

- In 2020 hebben nagenoeg alle gerechten rubricering op grond van de best practice rubricering ingericht. Datalekgevoelige informatie wordt steeds vaker gerubriceerd als hoog vertrouwelijk.
- De Baseline Informatiebeveiliging Overheid (BIO) wordt verder geïmplementeerd en gehanteerd.
- De werkgroep jij-bent-de-sleutel heeft verschillende initiatieven genomen om het bewustzijn te verhogen. Voor 2021 is een landelijke bewustwordingskalender opgesteld.

Incidentenregistratie

de Rechtspraak

	2018	2019	2020
Veiligheid	191	181	176
Agressie en geweld	houdt geen verband met woo-verzoek		
(incidenten) Bij zittingen buiten gerechtsgebouw			
(poging tot) Suïcide in cellengebied			
(poging tot) Uitbraak cellengebied			
(terroristische) Aanslag op de rechtspraak			
Schriftelijke agressie			
Email of social media (agressie)			
Fysiek met wapens			
Fysiek zonder wapens (handgemeen)			
Gijzeling			
Gooien met voorwerpen			
Mondeling/telefonisch (agressie)			
Vandalisme			
Bedrijfshulpverlening			
Besmettelijke ziekten			
Brand			
Bommelding			
Brandmelder (geactiveerd)			
Diverse			
Algehele spanningsuitval			
Diefstal			
Gas- en waterlekkage			
Schade door natuurverschijnselen (storm)			
Verdachte poststukken			

	2018	2019	2020
BEVEILIGING	148	180	88
Rijkspas	houdt geen verband met woo-verzoek		
Verlies doopkaarten			
Verloren rijkspassen			
Toegangscontrole			
Aanwezigheid pepperspray			
Aanwezigheid overige ongewenste goederen			
Aanwezigheid slag- en stootwapens			
Aanwezigheid steekwapens			
Aanwezigheid verboden geestbeïnvloedende middelen			
Aanwezigheid vuurwapens en/of munitie			
Overtreding minimumnorm toegangsverlening			
Vuurwerk aanwezig			
Overtreding (huis)regels			
Inbraak (/inbraak thuisadres)			
Onrechtmatig gebruik audiovisuele middelen			
Ordeverstoring			
Overtreding minimumnorm persrichtlijn			
Verlies van fysieke sleutels			
Integriteitsschending (nieuw sinds 2019)			

	2018	2019	2020
INFORMATIEBEVEILIGING	419	583	664
Datalek - gemeld AP	196	95	17
Datalek – gemeld PG-HR (Nieuw sinds 2019)	-	75	165
Datalek – gemeld AP en PG HR	-	0	10
Misbruik autorisaties	3	0	0
Overtreding minimumnorm email- en internetgebruik	1	0	0
Verlies gegevens (papier en digitaal)	213	398	457
IT-security			
Centrale ICT-uitval (langdurig)			
(poging tot) Hacking			
Lokale ICT-uitval			
Overtreding minimumnorm Rubricering			
Malware-besmetting			
(poging tot) Phishing			
Social engineering			
Externe meldingen a.g.v. Responsible Disclosure			

5.1(2)h

Verder opvallend in de incidentregistratie

Het jaar 2020 kenmerkt zich door:

- houdt geen verband met woo-verzoek [redacted]

- Een sterke stijging van de hoeveelheid verloren informatie.
  - Bij verloren informatie spreken we van informatie waarbij het waarschijnlijk is dat er geen inbreuk op de privacy van betrokkene heeft plaatsgevonden en die daarom niet in aanmerking komt voor melding aan de toezichthouders, maar desalniettemin wel nadelig is voor de Rechtspraak.
  - **Het minste verlies van informatie is gemeld door Gerechtshof 's-Hertogenbosch(0), Bureau Rvdr (1), Rechtbank Zeeland-West-Brabant (2) SSR (2) en IVO/LDCR (2)**
  - Het meeste verlies van informatie - is gemeld door het gerecht Midden-Nederland (88) en de Rechtbank Den Haag (70)

Verder opvallend in de incidentregistratie

- Een hoog aantal Datalekken
  - Het jaarlijks aantal datalekken (gemeld en niet gemeld) is ten opzichte van 2019 gestegen van 566 naar 649. Het aantal aan de toezichthouders gemelde datalekken is gestegen van 171 (2019) naar 192 (2020). In 2018 waren er 1.52 miljoen uitspraken en in 2019 1.54 miljoen uitspraken. 2020 is nog onbekend.
  - Als we spreken van Datalekken dan zijn dit de lekken die conform de AVG-verplichting gemeld zijn aan de toezichthouders: de Autoriteit Persoonsgegevens en of de Procureur Generaal bij de Hoge Raad. Een Datalek wordt gedefinieerd als het opzettelijk of onopzettelijk vrijgeven van beveiligde informatie aan een onvertrouwd publiek. In Nederland valt onrechtmatige verwerking of het verlies van gegevens ook onder een Datalek.
    - Het minste aantal Datalekken in 2020 is gemeld door het Bureau Rvdr (0) en het Studiecentrum Rechtspleging (SSR) (0) op korte voet gevolgd door de Rechtbank Noord-Holland, het Gerechtshof Amsterdam en de Centrale Raad van Beroep (allen 1)
    - De meeste datalekken in 2020 zijn gemeld door de Rechtbank Rotterdam (24) en de Rechtbank Overijssel (24)
  - Opvallend is de stijging in het aantal adresseringsfouten. Een adresseringsfout gaat verder dan het verkeerd (digitaal) opsturen van gegevens. Denk hierbij aan: persoon of bedrijf is niet langer gehuisvest in het aangeschreven pand.
- Aanbevelingen:
  1. Onderzoek de mogelijkheid om het unieke advocatennummer een grotere rol te laten spelen bij het koppelen van zaken.
  2. Leg op een duidelijke plek in het document vast om wat voor soort informatie het gaat, bijvoorbeeld op de voorkant of 2e pagina. Dit kan bijvoorbeeld door middel van het letterlijk benoemen of door het werken met kleurcodes. Hierdoor verlaag je de kans dat het over het hoofd wordt gezien.
  3. Bewustwording als continu proces.

Aspect	Aantal 2018	Aantal 2019	Aantal 2020
Adresseringsfouten	212	276	359
Anonimiseringsfouten	75	151	146
Verloren/zoek geraakt	43	49	35
Verwisseling gegevens	43	33	33
Bezorgfout	22	21	30
Autorisatiefout	12	28	24
Diefstal	13	7	6
Clean Desk	2	1	1

*Aantal 2020 in deze afbeelding is een momentopname van eind december 2020

Deelbesluit 1 - Datalekken
Document 21

de Rechtspraak
Raad voor de rechtspraak

Jaarverslag integrale veiligheid en beveiliging 2021

Bureau Beveiligingsautoriteit (voorheen Beveiligingsambtenaar)

de Rechtspraak
Raad voor de rechtspraak

De Beveiligingsautoriteit Rechtspraak (BVA) bewaakt het integrale karakter en de consistentie van de rechtspraakbrede kaders voor beveiliging en het toezicht op de werking van de integrale beveiliging van de rechtspraak.

de Rechtspraak
Raad voor de rechtspraak

Jaarverslag in cijfers

	2019	2020	2021
Veiligheid	181	176	352
Agressie en geweld	houdt geen verband met woo-verzo		
(incidenten) Bij zittingen buiten gerechtsgebouw			
(poging tot) Suïcide in cellengebied			
(poging tot) Uitbraak cellengebied			
(terroristische) Aanslag op de rechtspraak			
Schriftelijke agressie			
Email of social media (agressie)			
Fysiek met wapens			
Fysiek zonder wapens (handgemeen)			
Gijzeling			
Gooien met voorwerpen			
Mondeling/telefonisch (agressie)			
Doxing (nieuw sinds Q2 2021)			
Vandalisme/vernieling			
Bedrijfshulpverlening			
Besmettelijke ziekten			
Brand			
Bommelding			
Brandmelder/inbraakalarm (geactiveerd)			
Diverse			
Algehele spanningsuitval			
Diefstal			
Gas- en waterlekkage			
Schade door natuurverschijnselen (storm)			
Verdachte poststukken			

	2019	2020	2021
BEVEILIGING	180	88	130
Rijkspas	houdt geen verband met woo-verzoek		
Verlies doopkaarten			
Verloren rijkspassen			
Toegangscontrole			
Aanwezigheid pepperspray			
Aanwezigheid overige ongewenste goederen			
Aanwezigheid slag- en stootwapens			
Aanwezigheid steekwapens			
Aanwezigheid verboden geestbeïnvloedende middelen			
Aanwezigheid vuurwapens en/of munitie			
Overtreding minimumnorm toegangsverlening			
Vuurwerk aanwezig			
Overtreding (huis)regels			
Inbraak (/inbraak thuisadres)			
Onrechtmatig gebruik audiovisuele middelen			
Ordeverstoring			
Overtreding minimumnorm persrichtlijn			
Verlies van fysieke sleutels			
Integriteitsschending			

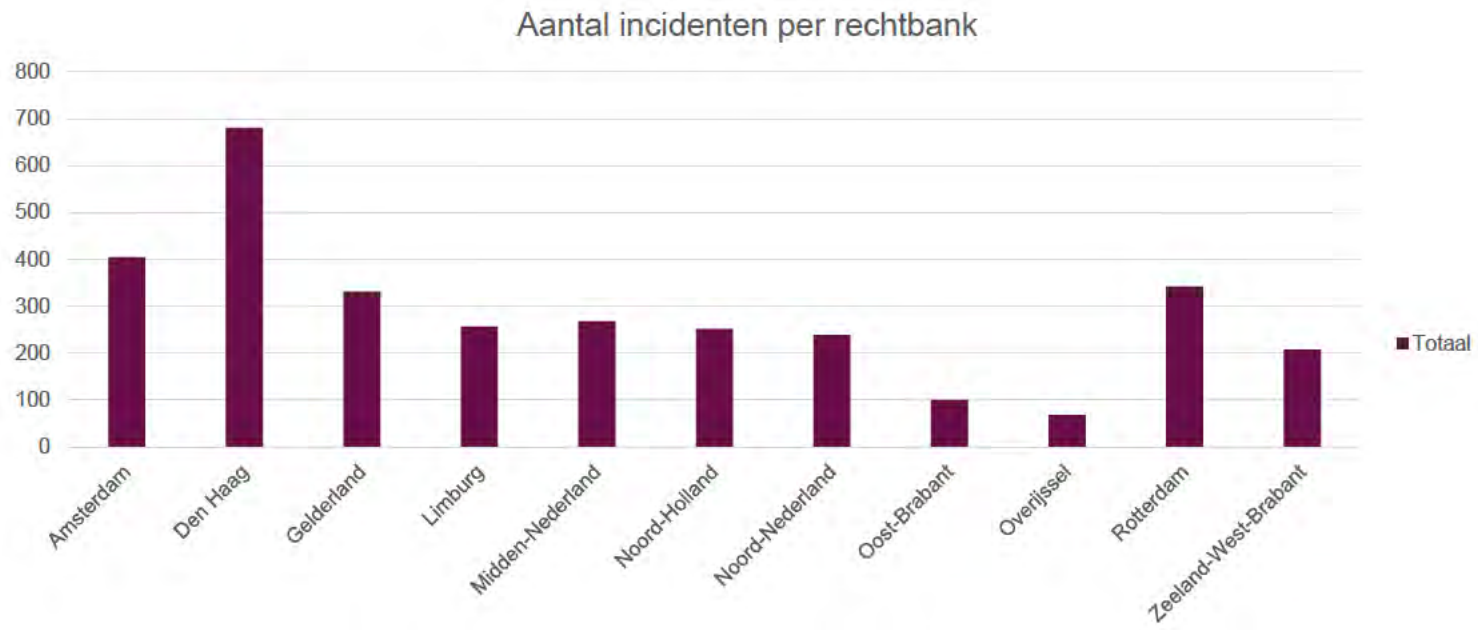
	2019	2020	2021
INFORMATIEBEVEILIGING	583	664	787
Datalek - gemeld AP	95	17	15
Datalek – gemeld PG-HR	75	165	196
Datalek – gemeld AP en PG HR	0	10	0
Misbruik autorisaties	0	0	2
Overtreding minimumnorm gebruik van digitale voorzieningen	0	0	0
Verlies gegevens (papier en digitaal)	398	457	555
IT-security			
ICT-uitval (langdurig)	5.1(2)h		
(poging tot) Hacking			
Lokale ICT-uitval			
Ddos-aanval (nieuw sinds Q2 2021)			
Overtreding minimumnorm Rubricering			
Malware-besmetting			
(poging tot) Phishing			
Social engineering			
Externe meldingen a.g.v. Responsible Disclosure			

Duiding van de incidenten en getroffen acties [2/2]

IT-security, diefstal en datalekken

- DDos-aanval legt een groot gedeelte van de Rechtspraak infrastructuur plat. De hinder duurde de gehele dag.
  - Actie: zoek meer de samenwerking met andere instanties (zoals het NCSC en J&V) om extra maatregelen te treffen om de kans op herhaling te beperken. IVO is hiermee reeds aan de slag.
- Het aantal diefstallen (op kantoor) is in de laatste vier maanden van 2021 voor het eerst gedaald naar nul meldingen. Dit is waarschijnlijk te danken aan het thuiswerken.
- Het aantal verlies van informatie – zonder meldplicht stijgt. Door het rechtspraakonderdeel is beslist dat de kans op schade of nadelige gevolgen voor de betrokkene wordt ingeschat op niet tot gering. De incidenten worden enkel intern vastgelegd, mede om aan de AVG te voldoen.
  - Actie: bewustwording om nauwkeurig en secuur werken te stimuleren. Dit is een doorlopende actie.

Uitgelicht: adresseringsfouten digitale postkamer [1/2]



de Rechtspraak
Raad voor de rechtspraak

Uitgelicht: adresseringsfouten digitale postkamer [2/2]

- De digitale postkamer is een systeem waarmee de administratie van een gerecht brieven, uitnodigingen en uitspraken aan partijen kan verstrekken. Dit is een systeem dat alleen bij rechtbanken draait.
- In december 2021 is geconstateerd dat via de digitale postkamer een groot aantal adresseringsfouten plaatsvindt. In de periode 10 februari 2020 tot 25 januari 2022 gaat het om 3153 incidenten. Deze incidenten waren in de meeste gevallen niet opgenomen in het incidentregistratiesysteem. In alle gevallen gaat het om datalekken, omdat persoonsgegevens aan een verkeerde persoon of organisatie zijn verstrekt. Een overzicht van de incidenten is gedeeld met de rechtbanken.
- Een kortetermijnmaatregel is op 7 februari 2022 in de digitale postkamer geïmplementeerd. Sindsdien zijn de aantallen aanzienlijk afgenomen. Incidenten beperken zich nu tot menselijke fouten van nieuwe en onervaren medewerkers. Aanvullend wordt in 2023 de lange termijn oplossing beschikbaar gesteld in de vorm van Digitaal Zaaksdossier.