Nr.	Naam
1	20180123 Presentatie AVG en Richtlijn - Beginselen en grondslagen op hoofdlijnen
2	20180123 Presentatie Privacy@Rechtspraak - Implementatie AVG en Richtlijn - Plan van aanpak
3	20180205 Presentatie Datalekken
4	20180313 Presentatie Privacy@Rechtspraak - Implementatie AVG en Richtlijn
5	20180522 Presentatie Implementatie AVG en Richtlijn - gegevensbescherming politie en justitie (Wjsg)
6	20180525 Handreiking verwerkersovereenkomsten (ten behoeve van inkoop)
7	20210913 Privacybeleid Rechtspraak
8	Interne Procedure Rechten Betrokkene
9	Poster ga zorgvuldig om met persoonsgegevens
10	Drie speerpunten en 10 gouden privacyregels

Document 1:
20180123 Presentatie AVG en Richtlijn - Beginselen en grondslagen op hoofdlijnen

AVG en Richtlijn Beginselen en grondslagen op hoofdlijnen

Bescherming persoonsgegevens

de Rechtspraak

Wat is privacy?

- “The right to be let alone”.
  - Warren & Brandeis, *Harvard Law Review 1890*

- Het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
  - Artikel 8 Europees Verdrag voor de Rechten van de Mens

Wat is gegevensbescherming?

- Het beschermen van persoonsgegevens die vanwege de manier waarop ze worden verwerkt, of vanwege hun aard of de context waarin ze worden gebruiken, een risico vormen voor privacy en individuele vrijheden.
  - OECD Privacy Principles

- De eerlijke verwerking van persoonsgegevens voor specifieke doeleinden op basis van toestemming of een andere legitieme grondslag. Het recht om de persoonsgegevens die zijn verzameld in te zien en het recht om deze te laten rectificeren.
  - Art. 8 Charter of Fundamental Rights EU

AVG en Richtlijn

de Rechtspraak

AVG is van toepassing op:

- De geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens van betrokkenen alsmede
- De verwerking van persoonsgegevens die in een bestand zijn opgenomen

Richtlijn is van toepassing op:

- de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of 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.

Verwerken

Elke bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens al dan niet uitgevoerd via geautomatiseerde procedés, zoals

- Verzamelen
- Vastleggen
- Ordenen
- Structureren
- Opslaan
- Bijwerken/wijzigen
- Opvragen
- Raadplegen
- Gebruiken
- Verstrekken/doorzenden
- Vernietigen
- Verspreiden/ter beschikking stellen
- Wissen
- Etc.

Verwerkingen

de Rechtspraak

Moeten

- rechtmatig, behoorlijk en transparant zijn
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden
- mogen niet verder worden verwerkt (doelbinding)
- toereikend, ter zake dienend en beperkt tot wat noodzakelijk is
- juist zijn en worden geactualiseerd indien nodig
- worden bewaard in een vorm die de opslag beperkt tot wat nodig is
- beveiligd worden door het nemen van passende technische en organisatorische maatregelen

Persoonsgegevens

Alle informatie over een ***geïdentificeerde*** of ***identificeerbare natuurlijke*** persoon

- Geïdentificeerd (direct):
  - Specifieke kenmerken: naam, adres, geboortedatum
  - Singling out

- Identificeerbaar (indirect):
  - te herleiden tot een persoon (BSN-nummer, stem, lichaamslengte, vingerafdruk, IP-adres)
  - de mogelijkheid om (zonder onevenredige inspanning) de identificatie tot stand te brengen door redelijk toegeruste verwerkingsverantwoordelijke

Bijzondere gegevens

- Persoonsgegevens waaruit *blijkt*:
  - Ras/etnische afkomst, politieke opvattingen, religieuze/levensbeschouwelijke overtuigingen, vakbondslidmaatschap
- Persoonsgegevens *met het oog op* de unieke identificatie van een persoon
  - Biometrische gegevens
- Gegevens *over/met betrekking op*
  - Gezondheid, seksueel gedrag, seksuele voorkeur
- Genetische gegevens
- Gegevens *betreffende*
  - Strafrechtelijke veroordelingen, strafbare feiten, veiligheidsmaatregelen

Gevoelige gegevens

- *Niet-bijzondere gegevens die – wanneer gelekt – mogelijk onder Bescherming persoonsgegevens vallen, een GEB/DPIA kunnen vereisen, en/of extra beveiligingsmaatregelen nodig hebben*
  - Profielen, voorspellingen, andere aspecten die het functioneren van de betrokkene op werk betreffen, economische situatie, gezondheid, persoonlijke voorkeuren en interesses, betrouwbaarheid of gedrag, locatie of beweging.
  - Gegevens verkregen via (systematische) monitoring of surveillance.
  - Gecombineerde/gekoppelde datasets
  - Inloggegevens
  - Gegevens betreffende een kwetsbare groep
    - Bijv. kinderen, werknemers, geestelijk zieken, asielzoekers, ouderen
  - Burgerservicenummer, officiële identiteitsinformatie

Beginselen (Artikel 5 AVG)

Het verwerken van persoonsgegevens is alleen toegestaan als de 6 beginselen van artikel 5 AVG, lid 1 in acht worden genomen:

a) De verwerking is ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant (“rechtmatigheid, behoorlijkheid en transparantie”);

b) Persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (“doelbinding”);

c) De persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is (“minimale gegevensverwerking”)

d) De persoonsgegevens moeten juist zijn en waar nodig worden geactualiseerd (“juistheid”)

e) De persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (“opslagbeperking”)

f) Een passende beveiliging van de persoonsgegevens is gewaarborgd (“integriteit en vertrouwelijkheid”)

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen (“verantwoordingsplicht”).

Uitzondering: algemeen belang, historisch, statistisch en wetenschappelijk onderzoek

AVG artikel 89, lid 1: “De verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met deze verordening voor de rechten en vrijheden van de betrokkene. Die waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.”

Samengevat: gegevens voor doeleinden van algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden voor langere tijd worden bewaard, dienen bij voorkeur geanonimiseerd of gepseudonimiseerd te worden. Zowel op het verstrekken van gegevens, het onderzoeken van gegevens en het bewaren van gegevens zijn de AVG en de Richtlijn nog van toepassing.

Rechtmatigheid Richtlijn

- verwerking is onder de richtlijn alleen rechtmatig bij;
  - een verwerking die noodzakelijk is voor de uitvoering van een taak door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of 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.

Basis regel

Elke verwerking moet;

Eén welbepaalde, uitdrukkelijk omschreven en ***gerechtvaardigde*** doelstelling hebben en

Verwerkt worden met een rechtmatige grondslag

Grondslagen

Toestemming

Vitale belangen

Wettelijke verplichting

Overeenkomst

Algemeen belang

Gerechtvaardigd belang

Beoordelen rechtmatigheid verwerking

- Is verwerking in lijn met de doelbinding waaronder de gegevens zijn verkregen.
- Is verwerking in lijn met de grondslag waaronder de gegevens verkregen zijn.
- Is verwerking helder en in duidelijke taal
- Past de verwerking bij de “Expectation of privacy”

Niet in lijn met doelbinding/grondslag dan is verwerking niet rechtmatig

Toestemming

- Geen rechtmatige grond voor overheidstaken.
- Toestemming moet het resultaat zijn van een actieve, geïnformeerde handeling en vrijelijk worden gegeven.
- Toestemming wordt gegeven voor één of meerdere omschreven doelen.
- Bij gezagsverhouding (werkgever-werknemer en overheid-burger) kan vrijelijk geven van toestemming in het geding zijn

Vitale belangen

- Alleen van toepassing bij vitaal belang betrokkene
- Een gegevensverwerking is gerechtvaardigd indien deze noodzakelijk is ter bestrijding van een ernstig gevaar voor de gezondheid van de betrokkene of een andere persoon.
- grondslag is alleen bedoeld om de fysieke integriteit of leven van de betrokkenen te waarborgen.
- naast de belangen van de direct betrokkene kunnen dit ook nog zaken als het monitoren van een epidemie en de verspreiding daarvan of in humanitaire noodsituaties, met name bij natuurrampen of door de mens veroorzaakte rampen zijn.

Wettelijke verplichting

- verwerkingen waarvoor geldt dat het niet mogelijk is een wettelijke plicht uit te voeren is zonder de verwerking van persoonsgegevens.
- Er moet een direct verband tussen het persoonsgegeven en de wettelijke plicht zijn.
- Voorbeeld: Kopie ID kaart in HR dossier

Overeenkomst

- Er is een overeenkomst tussen de verwerker en de betrokkene en voor deze overeenkomst is het verwerken van een aantal persoonsgegevens onontbeerlijk.
- de overeenkomst moet zelf niet gericht zijn op het verwerken van persoonsgegevens.
- altijd het logische gevolg of de logische voorwaarden voor de uitvoering van een overeenkomst/contract

Algemeen belang

- 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.

- persoonsgegevens slechts kunnen worden verwerkt met het oog op een vooraf vastgelegde wettelijke taak

Gerechtvaardigd belang

- Gerechtvaardigd belang is het resultaat van een afweging tussen de belangen van de organisatie, en de vrijheden van de betrokkenen.
- Gerechtvaardigd belang is nooit van toepassing op verwerking door een overheidsinstantie bij het uitoefenen van hun taken.

AVG en Richtlijn
Rechten betrokkenen

Bescherming persoonsgegevens

de Rechtspraak

Rechten betrokkenen

Recht op informatie

Recht om in te zien

Recht om te wijzigen

Recht om vergeten te worden

Recht om gegevens over te dragen

Recht op informatie

- Een betrokkene heeft recht op informatie als er gegevens van hem/haar verwerkt gaan worden
  - Principe van “reasonable expectancy of privacy” is belangrijk
- In beknopte, transparante, begrijpelijke en gemakkelijke en toegankelijke vorm.

- **Te verstrekken informatie** Artikel 15.

Recht op inzage

- Betrokkene heeft recht op inzag van zijn/haar gegevens
  - Verzoek moet binnen een maand zijn uitgevoerd
  - Verzoek mag geen inbreuk zijn op de privacy van een derde.

Recht om te wijzigen

- De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.

Recht om vergeten te worden

- Geen absoluut recht.

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld
- Bij intrekken toestemming
- Bij onrechtmatige verwerking
- Vanuit wettelijke verplichting

- Maar niet als:
  - voor het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting
  - om redenen van algemeen belang op het gebied van volksgezondheid
  - met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden
  - de instelling, uitoefening of onderbouwing van een rechtsvordering.

Beperking van de verwerking

- Verwerking moet worden gestopt als:

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene
- de verwerking is onrechtmatig
- Bij bezwaar gemaakt tegen de verwerking

Recht om gegevens over te dragen

- Verkrijgen gegevens in een gestructureerde, gangbare en machineleesbare formaat als:
  - Verwerking op grond van toestemming
  - Verwerking in het kader van de uitvoering van en overeenkomst

  - Verkrijgen gegevens mag geen inbreuk geven op de persoonlijke levenssfeer van een derde betrokkene

Document 2:
20180123 Presentatie Privacy@Rechtspraak - Implementatie AVG en Richtlijn - Plan van aanpak

de Rechtspraak

Privacy@Rechtspraak
Implementatie AVG en Richtlijn
Plan van aanpak

Structurele bescherming van persoonsgegevens van betrokkenen in rechtszaken en van het Rechtspraakpersoneel

Bescherming persoonsgegevens

Even voorstellen

de Rechtspraak

Het kernprojectteam

[redacted] (projectleider)
[redacted] (privacy adviseur)
[redacted] (communicatieadviseur)

Adviseurs

[redacted] (functionaris gegevensbescherming)
[redacted], [redacted] (landelijk beveiligingsambtenaar)
[redacted] (adviseur ICT en Recht)
[redacted] (adviseur ICT en Recht)
[redacted] (beleidsmedewerker/adviseur)

Inhoud programma

12.45-13.45	**Plan van aanpak**
13.45-14.00	Pauze
14.00-14.45	**Rechtmatigheid**
14.45-15.00	Pauze
15.00-15.45	**Workshop gegevensbescherming**
15.45-16.00	Pauze
16.00-17.00	**Reflectie en afronding**

AVG en Richtlijn, verschil met Wbp

de Rechtspraak

Artikel 24, lid 1 AVG

"Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen **aantonen** dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd."

Overige belangrijke punten:

- Betrokkenen krijgen meer rechten, recht om vergeten te worden;
- Specifieke eisen aan het verwerkingsregister;
- Privacy impact Assessment en Privacy by design / by default;
- Actief gegevensbeschermingsbeleid en privacyverklaring;
- Verwerkersovereenkomsten;
- Uniformering binnen Europa, strenger boetebeleid.

Voor het strafrecht is er een aparte Richtlijn met strengere eisen aan de beveiliging, met name loggingsvereiste.

Stand van zaken I

de Rechtspraak

Strategisch plan (september 2017)

Visie op privacy is omarmd door Raad en PRO.

Governance

Wij beschikken al jaren over een uitstekende functionaris gegevensbescherming. IVO is bezig een fulltime Privacy Officer te werven. Structurele inbedding bij gerechten.

Datalekbeleid

Datalekbeleid met een functionerend datalekteam.

Centrale IT applicaties

Vooronderzoek door IVO beheerde IT applicaties afgerond.

Werkgroep is bezig de centrale IT applicaties in kaart te brengen (inclusief bedrijfsvoeringsapplicaties zoals Leonardo).

Rechtspraakpersoneel

Deelproject voor gegevensbescherming Rechtspraakpersoneel (inclusief schonen dossiers) wordt via HRM afdelingen uitgerold.

Stand van zaken II

de Rechtspraak

Verwerkersovereenkomsten

IVO inventariseert IT contracten en past waar nodig aan.

LDCR inventariseert raamcontracten en past waar nodig aan.

Interne bewustwording, rechten betrokkenen en communicatie

Een projectgroep is bezig met een communicatieplan.

Uitrol procedure en protocollen voor rechten betrokkenen.

Aanpassen rechtspraak.nl

Gegevensbeschermingsbeleid en privacyverklaring

Een projectgroep is bezig het gegevensbeschermingsbeleid op te stellen. Dit zal ter review worden voorgelegd aan belanghebbenden en in april/mei ter instemming aan Raad en PRO worden voorgelegd.

Stand van zaken III

de Rechtspraak

Connecting the dots: pilot bij een gerecht

Voor één gerecht alle verwerkingen en maatregelen in kaart brengen, beleid, procedures en normenkaders optimaliseren en vervolgens een best practice model ontwikkelen voor de Rechtspraak.

Wat vragen wij van de gerechten?

Lijst van lokaal beheerde IT applicaties

Afwijkende processen op lokaal (bv. lok. Deskundigenreg. naast DIX)

Lokale contracten

<u>Hier gaat het projectteam ondersteuning bieden</u>

In kaart brengen lokale verwerkingen en maatregelen (register)

Waar nodig aanpassen en optimaliseren van maatregelen

Handreikingen, procedures, factsheets, checklists

Door het projectteam worden deze geproduceerd en ter beschikking gesteld via Intro. Wij vragen ook van gerechten en diensten hun kennis en informatie te delen.

Deelprojecten

- Governance en toezicht
- Gegevensbeschermingsbeleid en privacyverklaring (inclusief handreikingen, procedurebeschrijvingen en factsheets)
- Landelijk register voor gerechten (met lokale afgeleiden)
- Interne bewustwording en externe communicatie
- Centrale IT applicaties IVO
- Landelijke informatievoorziening LDCR
- Privacy Rechtspraakpersoneel
- Verwerkersovereenkomsten
- Lokale registers diensten (LDCR, IVO, SSR en bureau)

Globaal tijdspad

November/december	Voorbereiding, passen en meten
23 januari	**Eerste themamiddag aanspreekpunten gerechten en diensten**
Februari	Handreikingen, procedures en factsheets worden gedeeld met aanspreekpunten.
Maandag 05 maart	**Informeren PRO over voortgang**
Half maart	**Concept landelijk verwerkingsregister gereed**
13 maart	**Tweede themamiddag aanspreekpunten**
April/mei	**Raad en PRO stemmen in met gegevens-beschermingsbeleid en de privacyverklaring.**
28 april	**Landelijk verwerkingsregister compleet**
Medio mei	**Derde themamiddag aanspreekpunten gerechten**
Vrijdag 25 mei	**Online publicatie Privacyverklaring Rechtspraak & AVG-borrel**
Juni	Eindrapportage en décharge door Raad
Juli/augustus	Nazorg en definitieve borging binnen de IC-cyclus.

Contact en informatie

de Rechtspraak

Contact

Vragen over de implementatie AVG en Richtlijn kunt u stellen aan de projectleider, Rick Goedkoop. Verder kunt u altijd terecht bij een van de andere adviseurs met een specifiek inhoudelijke vraag over een bepaald onderwerp.

Landelijke Intropagina

Medio februari wordt een landelijke Intropagina gelanceerd met informatie over het project onder de kop “projecten”

Teamsite

Medio februari worden via een teamsite handreikingen, procedurebeschrijvingen en factsheets gedeeld. Wij vragen ook aan u uw kennis en informatie te delen via Mijn Kennisomgeving.

Dialoog en consensus

Samenwerking en actieplannen komen tot stand op basis van dialoog en consensus. Als u mee wilt denken of doen, bent u van harte welkom. Als u beschikt over lokale registers, handreikingen, procedurebeschrijving of factsheets: deel deze vooral met ons.

Strategische visie en hoofdlijnen

de Rechtspraak

23 januari 2018

Missie

De Rechtspraak verwerkt persoonsgegevens op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.

De Rechtspraak leeft de Wbp reeds na. Er ligt een goede basis (wet meldplicht datalekken, reeds conform AVG).

Het project implementatie AVG en Richtlijn draagt eraan bij deze missie gestalte te geven en streeft naar verdere optimalisering en professionalisering.

Raad en PRO stellen gegevensbeschermingsbeleid en de publieke privacyverklaring Rechtspraak vast.

De Rechtspraak is transparant over welke persoonsgegevens zij verwerkt voor welke doelen en welke maatregelen worden getroffen teneinde de persoonsgegevens te beschermen.

Visie

de Rechtspraak

Strategie

Bescherming persoonsgegevens is een bestuurlijke prioriteit.

Structuur

Taken, verantwoordelijkheden en bevoegdheden met betrekking tot bescherming persoonsgegevens zijn belegd.

Cultuur

Medewerkers op alle niveau's binnen de organisatie zijn zich bewust van risico's en beschikken over kennis, vaardigheden en informatie.

Systeem

Er is een systeem van organisatorische en technische maatregelen welke in samenhang de bescherming van persoonsgegevens borgen en de adequate werking van dit systeem wordt gecontroleerd.

Sterkten en zwakten, kansen en bedreigingen

de Rechtspraak

Sterkten

De Rechtspraak is al langer vertrouwd met de bescherming van persoonsgegevens. Er is een integraal beleid voor fysieke en informatiebeveiliging dat ook gericht is op bescherming van vertrouwelijke dossiers, meldplicht datalekken werkt naar behoren.

Zwakten

De Rechtspraak heeft even als vele andere organisaties minder ervaring met digitaal werken.

Kansen

Het optimaliseren van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens heeft positieve gevolgen voor de kwaliteit van werkprocessen (minder fouten, verlies, etc.).

Bedreigingen

Ongeoorloofd of onopzettelijk verlies, diefstal, wijziging, verwijdering, toegang, verstrekking, cybercrime, etc.

Strategisch plan privacy
(Raad en PRO, september 2017)

de Rechtspraak

Strategie

Hoe gevoeliger de gegevens, hoe hoger het ambitieniveau.

Ambitieniveau ligt hoger voor primair proces dan bedrijfsvoering.

Structuur

Functionaris gegevensbescherming bij de Rvdr. Privacy Officer voor IVO en LDCR. Aanspreekpunten bij gerechten. Uiteindelijke structuur voor Raad, gerechten en diensten nog nader bepalen.

Cultuur

Bewustwording, communicatie en educatie is van groot belang.

Systemen

Organisatorische en technische maatregelen dienen op orde gebracht te worden. Privacy Impact Assessment staat centraal.

Project implementatie AVG en Richtlijn

Het strategisch plan wordt verder uitgewerkt in het project.

Nadere toelichting op een aantal onderdelen

Gegevensbeschermingsbeleid en privacyverklaring

de Rechtspraak

De Rechtspraak is transparant over de verwerking van persoonsgegevens en de organisatorische en technische maatregelen welke worden getroffen teneinde de persoonsgegevens in overeenstemming met de AVG en de Richtlijn Straf te beschermen.

Hiermee verkleinen we het risico op onterechte inbreuk op de persoonlijke levenssfeer van betrokkenen.

April/mei	Raad en PRO stemmen in met het gegevensbeschermingsbeleid en de privacyverklaring voor de Rechtspraak.

Landelijk verwerkingsregister

de Rechtspraak

Vanuit het project is een model ontwikkeld voor het in kaart brengen van verwerkingen in centrale IT applicaties.

Voor de gerechten zal op korte termijn in samenwerking met een projectgroep van een rechtbank een model ontwikkeld worden voor gerechten wat grotendeels al ingevuld zal worden voor de gerechten. Uitgangspunt is dat een groot deel van de processen (straf, civiel, bestuur, personeel, facilitair, financiën) een overeenkomstig verloop kennen

Vervolgens wordt aan gerechten gevraagd het model aan te passen en waar nodig aan te vullen aan de lokale situatie.

Verwerkingsregister in het kort:

- Processen en systemen
- Categorieën persoonsgegevens
- Doeleinden en grondslagen
- Verzameling van persoonsgegevens (betrokken partijen)
- Verstrekking van persoonsgegevens (betrokken partijen)
- Bewaartermijnen
- Maatregelen

Inkoop: verwerkersovereenkomsten

Contracten met leveranciers welke toegang hebben tot persoonsgegevens moeten mogelijk aangepast worden.

Voor verwerkersovereenkomsten wordt geadviseerd het **"model verwerkersovereenkomst Rijk"** (ARVODI of ARBIT) te hanteren.

Hiervoor is een checklist ontwikkeld vanuit het Rijk welke op korte termijn voor de Rechtspraak geschikt zal worden gemaakt.

Rol functionaris gegevensbescherming

Nieuwe contractaanpassingen en verwerkersovereenkomsten ter toetsing voorleggen in het kader van de adviesbevoegdheid.

Acties centraal

LDCR inventariseert raamcontracten en past indien nodig aan.

LDCR coördineert ook de aanpassing van nadere overeenkomsten.

Spir-it inventariseert door spir-it beheerde IT contracten

Acties decentraal

Lokale overeenkomsten inventariseren en indien nodig aanpassen.

Coördinatie verloopt via LDCR in samenwerking met het projectteam.

Rechtspraakpersoneel

de Rechtspraak

Apart deelproject, loopt via HRM afdelingen gerechten.

Acties centraal

Centrale IT applicaties worden door LDCR en spir-it in kaart gebracht. Voor P-direkt wordt BZK benaderd.

Acties decentraal

Er wordt op korte termijn een apart deelproject opgestart met een projectgroep. Vervolgens zullen de HRM afdelingen benaderd worden.

Nadere informatie volgt.

Interne controle en auditing

de Rechtspraak

Nadat het beleid, de procedures en normenkaders zijn uitgekristalliseerd, zal via de P&C-afdelingen de interne controle en auditing-beleid verder vorm gegeven worden.

Deliverables

Ondermeer: intern controleplan en vragenlijst.

Planning

Start in juni. Gerechten worden via het LCO geïnformeerd.

Document 3:
20180205 Presentatie Datalekken

Datalekken

Datalekteam, Raad voor de rechtspraak

Even voorstellen

[redacted]

- Senior juridisch adviseur
- Afdeling HRM & OO
- Functionaris gegevensbescherming
- Lid van het datalekteam

Het kernprojectteam AVG

[redacted] (projectleider)
[redacted] (extern privacy adviseur)
[redacted] (communicatieadviseur)

Adviseurs AVG

[redacted] (functionaris gegevensbescherming)
[redacted] [redacted] (landelijk beveiligingsambtenaar)
[redacted] (adviseur ICT en Recht)
[redacted] (beleidsondersteunend medewerker ICT en Recht)

Privacy

Toenemend belang privacy

- Door digitalisering van de samenleving, steeds meer aandacht voor privacy.
- 25 mei 2018: nieuw Europees privacykader van toepassing:
  - ❑ Algemene verordening gegevensbescherming (“AVG”)
  - ❑ Wet bescherming persoonsgegevens (“Wbp”) vervalt!
  - ❑ Richtlijn bescherming persoonsgegevens opsporing en vervolging: implementatie in Wpg en **Wjsg**

Meldplicht datalekken

- Sinds 1 januari 2016 Wet meldplicht datalekken in Nederland van kracht. Opgenomen in de Wbp
- Vooruitlopend op de meldplicht die is opgenomen in de AVG.
- Doel + ratio Meldplicht datalekken.

Verschil Wbp/AVG+Richtlijn

Artikel 24, lid 1 AVG

"Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen **aantonen** dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd."

Nieuwe wettelijke vereisten privacy:

- Het voeren van een actief gegevensbeschermingsbeleid;
- Het documenteren van gegevensverwerkingen;
- Het uitvoeren van een Privacy Impact Assessment *(PIA*);
- De aanstelling van een Functionaris Gegevensbescherming;
- Het toepassen van *privacy by design/privacy by default;*
- Afspraken tussen verwerkers – aansprakelijkheid van verwerkers;
- Uitbreiding rechten van betrokken (oa recht op vergetelheid);
- Het bijhouden van logbestanden (uitsluitend Richtlijn).
- Uniformering binnen Europa, strenger boetebeleid.

Persoonsgegevens

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene).

Gewone persoonsgegevens
Een persoon is identificeerbaar als hij direct of indirect geïdentificeerd kan worden aan de hand van één of meerdere gegevens, zoals NAW-gegevens, geboortedatum, telefoonnummer, IP-adres. Gegevens die over een persoon gaan, dan wel naar een natuurlijk persoon te herleiden zijn vallen binnen de privacywetgeving.

Gevoelige persoonsgegevens
Een aantal persoonsgegevens worden als gevoelig aangemerkt, dit zijn bijvoorbeeld financiële gegevens, het BSN, locatiegegevens, gegevens m.b.t. kinderen of andere kwetsbare groepen. Deze gegevens kunnen in potentie meer bedreiging vormen voor de persoonlijke levenssfeer van betrokkenen.

Bijzondere persoonsgegevens
Voor het verwerken van bijzondere persoonsgegevens geldt een verwerkingsverbod. Gegevens betreffende iemands ras, gezondheid, seksuele leven, politieke voorkeur, genetische gegevens en biometrische gegevens zijn bijzondere gegevens. Maar ook strafrechtelijke gegevens zijn aan een apart regime gebonden. Deze gegevens mogen alleen verwerkt worden als daarvoor een uitzondering bestaat in de privacywetgeving.

De wettelijke meldplicht

Tweetrapsraket:

Melding aan Autoriteit Persoonsgegevens

Artikel 34a lid 1 Wbp: de **verantwoordelijke** stelt het College (nu: Autoriteit Persoonsgegevens "AP") **onverwijld**, maar uiterlijk binnen 72 uur, in kennis van een **inbreuk op de beveiliging** die leidt tot de **aanzienlijke kans** op ernstige nadelige gevolgen dan wel ernstige **nadelige gevolgen** heeft voor de bescherming van persoonsgegevens. (= artikel 33 AVG)

Ja / Ja Ja / Nee

Melding aan betrokkene

Art. 34a lid 2 Wbp: de **verantwoordelijke** stelt de **betrokkene onverwijld** in kennis van de **inbreuk**, indien de inbreuk **waarschijnlijk ongunstige gevolgen** zal hebben voor diens persoonlijke levenssfeer. (= artikel 34 AVG)


Beveiligingsincident
Datalek
•Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?
Melden aan de Autoriteit Persoonsgegevens
•Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?
Vraag advies aan het datalekteam
72 uur
Melden aan de betrokkene
•Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?
Documenteren en versturen naar het Datalekteam
•Documenteer alle datalekken en stuur de meldingen en ontvangstbevestigingen naar het Datalekteam.

Niet voldoen aan de meldplicht

Hoge boetes

- Onder huidig recht kan Autoriteit Persoonsgegevens boetes opleggen die kunnen oplopen tot *€ 820.000!*
- Onder AVG kan de Autoriteit Persoonsgegevens boetes opleggen die kunnen oplopen tot *€ 10 miljoen!*
- *Thans nog geen expliciete boetemaxima vastgelegd in de Richtlijn; de vaststelling hiervan wordt overgelaten aan lidstaten. Zal geregeld worden in de Wpg en Wjsg.*

Niet voldoen aan de meldplicht

Reputatieschade

10 februari 2017 07:37

'Bouwvakkers vinden gevoelige dossiers bij sloop rechtbank Amsterdam'

'Datalek' bij rechtbank Breda, USB-sticks in post verloren

21 januari 2017 | Laatste update: 21 januari, 06:00

1 REAGEER (9)

Datalek: OM kan kijken bij rechters

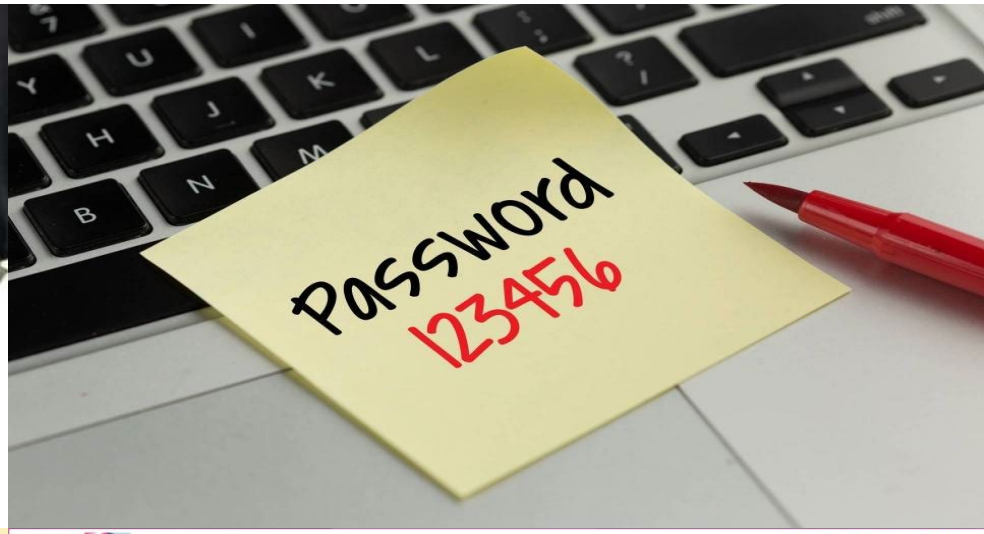
Rechterlijk computersysteem

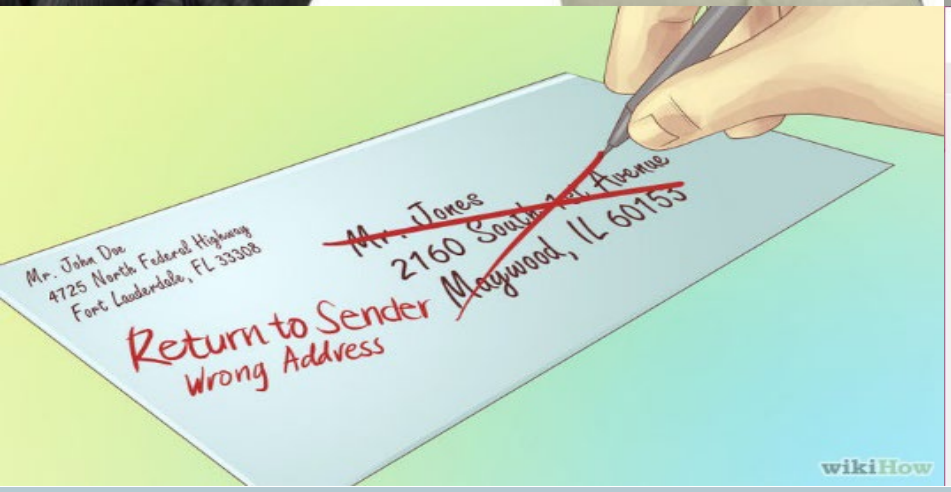
Door te ruime verstrekking van autorisatiecodes konden OM-medewerkers vonnissen lezen in grote drugszaak nog voordat deze waren uitgesproken.

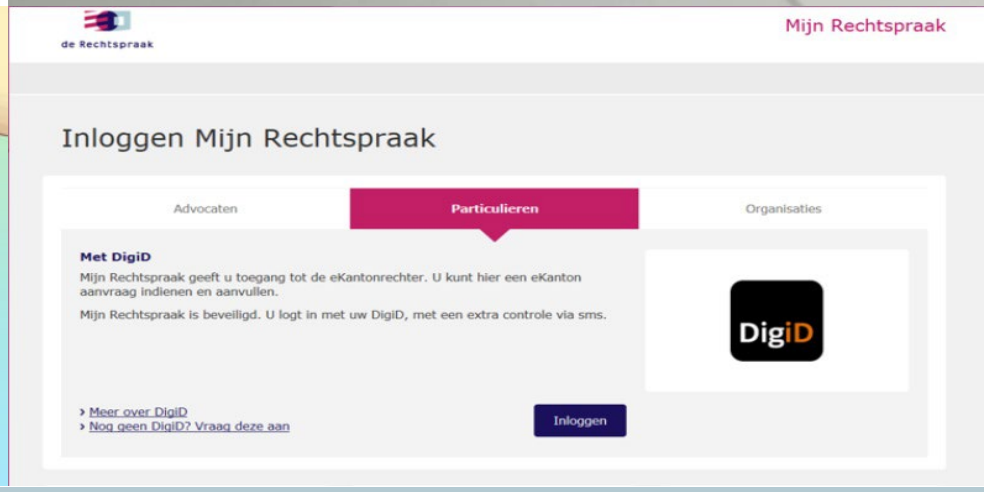
Marcel Haenen 10 juni 2017

In het computersysteem van de rechterlijke macht ('Compas') is een ernstig datalek geconstateerd. Medewerkers van het Openbaar Ministerie blijken in sommige gevallen

Voorbeelden datalekken?







Datalekken in de Rechtspraak-praktijk

Veelvoorkomende datalekken

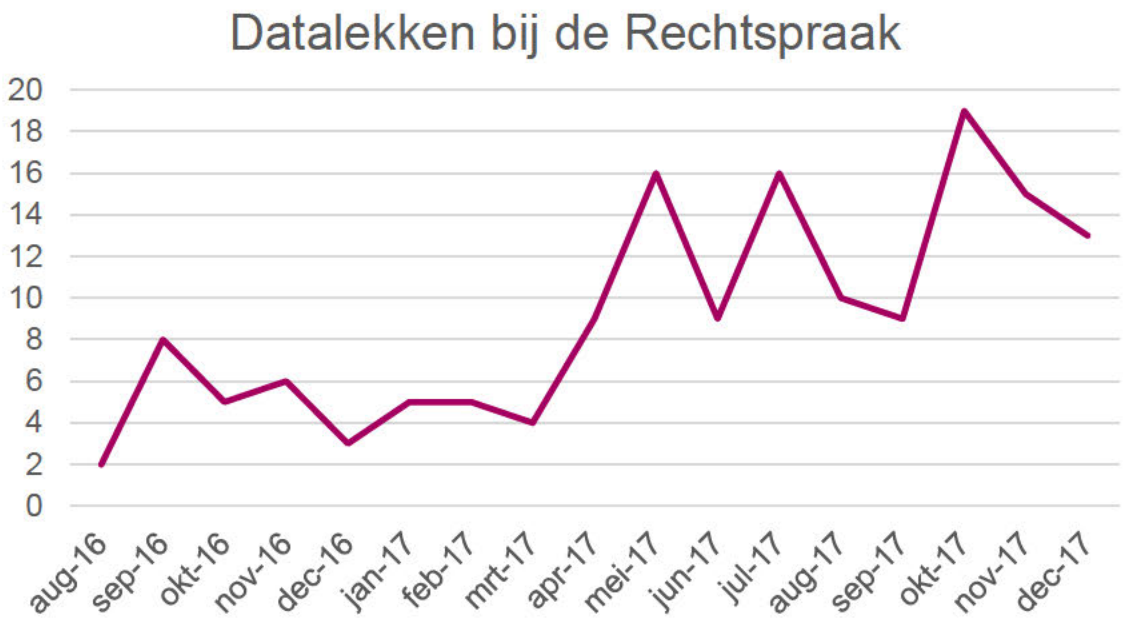
- (Proces)stukken die worden verzonden aan personen die niet bevoegd waren daartoe inzage te hebben;
- Diefstal van of verloren geraakte gegevensdragers (iPad, laptop, telefoon, USB);
- Het per abuis toevoegen van processtukken aan een onjuiste gemachtigde in één van de digitale webportalen (ontwikkeling van werkprocessen);
- Poststukken die niet aankomen bij geadresseerden, dan wel foutief worden bezorgd of verloren raken;
- (Proces)stukken die worden verzonden aan foutieve e-mailadressen;
- Per abuis publiceren van persoonsgegevens in uitspraken op rechtspraak.nl.

Of er sprake is van een datalek, is uiteraard afhankelijk van de omstandigheden van het geval.

Wat doet het datalekteam

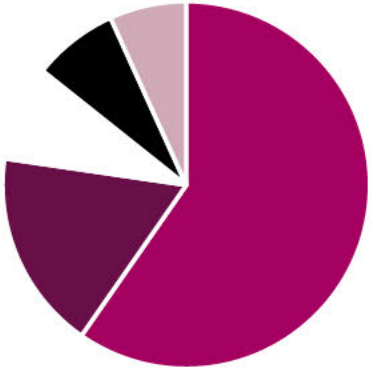
- Kees Sterk (portefeuillehouder privacy & informatiebeveiliging) en Peter Arnoldus (fysieke informatiebeveiliging).
- Handboek Meldplicht datalekken voor gerechten en leaflet datalekken.
- Verlenen (eerste hulp) advies aan gerechten en landelijke diensten bij een datalek: datalekteam.rvdr@rechtspraak.nl.
- Verlenen advies over de juridische interpretatie van de Meldplicht datalekken.
- De meldingen van voorgevallen datalekken bij landelijke diensten bij de Autoriteit Persoonsgegevens.
- Het documenteren van alle datalekken vindt per 1 januari 2018 plaats in Classbase.

Gegevens Datalekteam



In 2017 waren 128 meldingen.
In 76 incidenten zijn de betrokkenen geïnformeerd.
Het totaal aantal betrokkenen dat een melding heeft ontvangen is 560 en dat is gemiddeld 7,6 persoon per incident.

Oorzaken Datalekken



- 55.5% poststuk of email was foutief geadresseerd
- 16.4% object gestolen of kwijt
- 7.8% probleem veroorzaakt tijdens verzending van het poststuk
- 7% foutieve publicatie van gegevens
- 6.3% probleem bij IT

Vraagstukken / dilemma's

Na het publiceren van een uitspraak op rechtspraak.nl neemt een advocaat contact op dat de naam van zijn cliënt nog zichtbaar is in de uitspraak. Wat zijn de vervolgstappen en is de meldplicht datalekken van toepassing?

Zou de beoordeling anders zijn als enkel het adres van cliënt zichtbaar was geweest in de uitspraak?

Je stuurt een gevoelig document per e-mail naar een collega. Na het versturen kom je erachter dat er per ongeluk een fout in het e-mailadres is geslopen. De e-mail met het gevoelige document is bij een collega van een ander arrondissement terecht gekomen. Is hier sprake van een datalek?

Bevat je mobiele telefoon persoonsgegevens?

Zo ja: Wat doe je als je mobiele telefoon wordt gestolen?

Moet er ook altijd een melding aan betrokkenen worden gedaan?

Document 4:
20180313 Presentatie Privacy@Rechtspraak - Implementatie AVG en Richtlijn

de Rechtspraak

Privacy@Rechtspraak
Implementatie AVG en Richtlijn

Structurele bescherming van persoonsgegevens van betrokkenen in rechtszaken en van personele en overige gegevens

Welkom

Agenda

12:00 - 13:00	Inloop/lunch
13:00 - 13:15	Welkom
13:20 - 13:45	Update programma
13:50 - 15:15	Privacy management deel I
15:15 - 15:30	Pauze
15:30 - 16:30	Privacy management deel II
16:30 - 17:00	Afronding

Update landelijk programma

Landelijk register van verwerkingen (vóór 28 april gereed):

- Inventarisatie centrale IT applicaties (inclusief beveiliging)
- Modelregister voor de gerechten;

Inkoopcontracten

- Inventarisatie landelijke raamcontracten en IT contracten;

Beleid

- PRO 09 april: governance en toezicht
- PRO 14 mei: gegevensbeschermingsbeleid

Handreikingen en factsheets

Komende vrijdag of maandag op Intro Landelijk.

Privacyverklaring Rechtspraak

Een heldere uitleg aan betrokkenen.

Wat vragen wij van de gerechten en diensten vóór 28 april 2018?

1. Lokale inventarisaties IT applicaties

Maak een lijst met **lokale** IT applicaties waarin persoonsgegevens worden verwerkt en omschrijf kort welke persoonsgegevens worden verwerkt.

2. Lokale inventarisatie inkoopcontracten

Maak een lijst met lokale inkoopcontracten waarin persoonsgegevens verwerkt en omschrijf kort welke persoonsgegevens worden verwerkt.

3. Lokale inventarisaties documenten en lijsten

Maak een lijst met lokale document/lijsten waarin persoonsgegevens worden verwerkt en omschrijf kort welke persoonsgegevens worden verwerkt.

Terug rapporteren aan het projectteam op 28 april.

Het projectteam zal daarna adviseren over vervolgstappen.

Pro memorie: verwerkingen HRM en financiën.

Wat vragen wij van de gerechten en diensten na 25 mei 2018?

1. Implementeer privacy governance binnen uw organisatie

Privacy coördinatoren, hoofden afdelingen/teams, contactpersonen afdelingen/teams.

2. Voer een actief gegevensbeschermingsbeleid

Zorg ervoor dat de privacyregels worden gevolgd binnen het gerecht.

3. Implementeer een PDCA-cyclus

Zorg voor blijvende verbetering door periodieke evaluaties met actieplannen.

De derde themamiddag (eind april) zal in het teken staan van het concreet doorvoeren van bovenstaande en vooral het stimuleren van bewustwording binnen de gerecht en diensten.

Drie speerpunten en 10 regels

1. Toegang (jij bent de sleutel)

1.1 Beperk autorisatie medewerkers tot noodzaak.

1.2 Let op clean desk policy, gesloten ruimten en kasten

1.3 Let op e-mail en internet gebruik, USB-sticks, thuiswerken.

2. Verstrekking

Verstrek alleen gegevens na:

2.1 Vaststelling wettelijke grondslag.

2.2 Vaststelling identiteit van de betrokkene.

2.3 Vaststelling bevoegdheid verzoeker.

En:

2.4 Bescherm privacy anderen in dossiers en registraties.

3. Registreren en bewaren

3.1 Verwerk niet meer dan nodig.

3.2 Bewaar niet langer dan nodig, vernietig als kan.

3.3 Beperk herleidbaarheid tot individu: door gegevens (NAW) uit een bestand te verwijderen, door anonimisering.

Wbp versus AVG

Een korte opfrisser

aanvullende sheets

de Rechtspraak

Wbp en AVG – overeenkomsten

Informatieplicht	Transparantie t.a.v. gegevensverwerking / verstrekken informatie aan betrokkene.
Recht- en doelmatigheid	Grondslag en doel voor verwerking (o.g.v. toestemming, wettelijke verplichting of vervulling taak.
Duur	Niet langer dan noodzakelijk, daarna verwijderen.
Noodzakelijkheid	Verwerking voor zover strikt noodzakelijk.
Waarborgen	Technische en organisatorische bescherming processen / systemen. Let op: bijv. versturen van processtukken per e-mail biedt onvoldoende waarborgen.
Profilering	Recht om niet automatisch zonder menselijke tussenkomst onderworpen te worden aan besluiten met juridische gevolgen.

Wbp en AVG – veranderingen I

▪ **Toepassingsbereik**	Ook instanties buiten de EU persoonsgegeven verwerken van EU burgers.
▪ **Recht op vergetelheid**	Sterker recht om ‘vergeten te worden’.
▪ **Data portabiliteit**	Persoonsgegevens dienen overdraagbaar te zijn / Recht op kopie.
▪ **Verwerkingsregister**	Eigen register vervangt algemene registratieplicht AP.
▪ **Privacy by design /default**	Reeds bij ontwerpfase van nieuwe processen aandacht voor privacy.

Wbp en AVG – veranderingen II

- **Beperkingen** — Strengere eisen aan verwerking van bijzondere gegevens (bijv. biometrische).
- **Datalekken** — Inbreuken melden bij AP.
- **FG** — Sneller Functionaris Gegevensbescherming vereist.
- **Verwerkersverantwoordelijke** — (1) Degene die de doeleinden en middelen bepaalt is verantwoordelijke. (2) Delegatie mogelijk mits bescherming gegevens is geborgd. (3) Bij meerdere verantwoordelijken dienen duidelijke en transparante afspraken te zijn gemaakt.
- **Sancties** — Sanctionering op overtreding Bevoegdheden AP zwaarder.

de Rechtspraak

Privacy management, deel I

PDCA en Governance

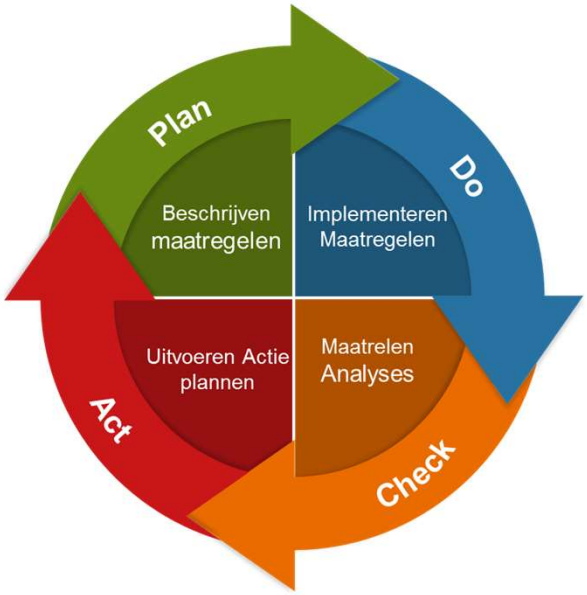
PDCA en de AVG

Artikel 24, lid 1 AVG

“Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, **treft (PLAN)** de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt **uitgevoerd (DO)**. Die maatregelen worden **geëvalueerd (CHECK)** en indien nodig **geactualiseerd (ACT)**.”

PDCA cyclus

- Om aantoonbaar in control te zijn en te blijven is de implementatie van een PDCA cyclus voor Privacy management nodig. (art24)
- Niet 1 keer bedenken en dan vergeten, maar constante (periodieke) evaluatie, heroverweging en aanpassing.
- Privacy actieplan maken met specifieke acties, als levend document. **Format actieplan.**



Plan
Verwerkingen zijn geinventariseerd en beschreven. Beleid en maatregelen worden beschreven

Do
Maatregelen worden uitgevoerd, en zijn in werking.

Check
Effectiviteits- en volledigheidsbeoordelingen vinden plaats.

Act
Gaps worden omgezet in acties, controles leiden tot verbeteringen

Levenscyclus van Informatie

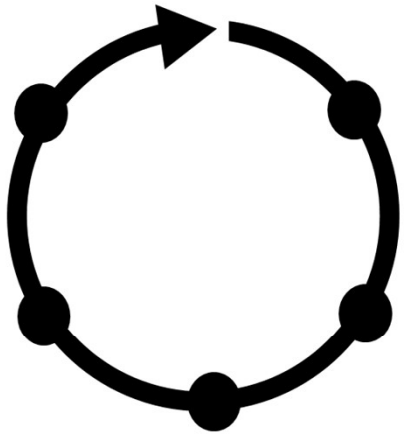
- Elke fase uit de levenscyclus van een gegeven geeft input voor het beheersproces

Destruction

Guidelines on how to destroy the data based on its type should exist

Retention

The persistence of data by an organization after its collection



Disclosure

Internal, external, according to legal obligations and notice

Collection

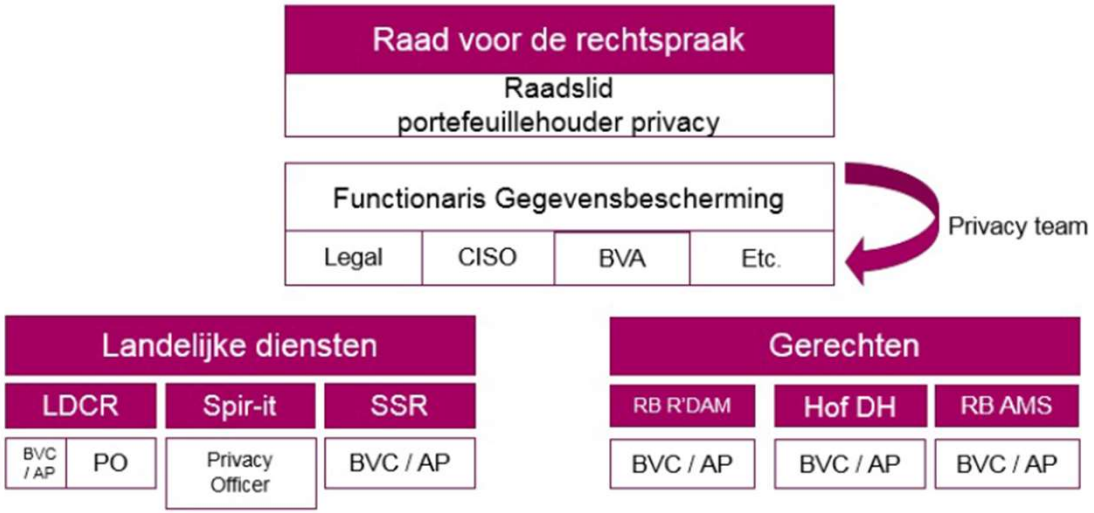
The process of receiving data from a user, device or entity

Use

Processing or sharing of information beyond simple storage and deletion

GOVERNANCE EN TOEZICHT

Zoals in Strategisch plan privacy



AP = aanspreekpunt privacy
PO = privacy officer

Functionaris gegevensbescherming

De Functionaris gegevensbescherming (FG) heeft vanuit AVG art, 39 de volgende taken:

- Informeert over de AVG
- Ziet toe op de naleving van de AVG
- Geeft gevraagd en ongevraagd advies
- Werkt samen met de externe toezichthouder
- Is contactpunt voor toezichthouder

- Praktisch betekent dit;
  - Dwingend advies geven over uitgevoerde PIA's
  - Toezicht houden op volledigheid registers
  - Toezicht houden op werking datalek meld proces
  - Advies geven over voorgenomen verwerkingen

Wanneer FG betrekken:

- Uitvoeren PIA, advies over rechtmatigheid en beveiliging, datalekken

Privacy Officer IVO

150+ centrale IT applicaties en nieuwe applicaties:

- Ondersteunen bij privacyanalyses waaronder het aanwijzen van passende beheersmaatregelen
- Ontwikkelen van toegepast privacybeleid en -procedures
- Stimuleren van bewustwording en training van medewerkers van de centrale organisatie
- Voeren van incidentmanagement met betrekking tot datagerelateerde incidenten
- Opstellen van een werkprogramma/ jaarplan met betrekking tot privacy
- Monitoren en rapporteren over de uitvoering van het beleid en het werkprogramma
- Evalueren van het privacy beleidskader en doen van aanbevelingen over wijzigingen ten aanzien daarvan.
- Gericht op de centrale (IT) verwerkingen

Advies lokale privacy governance

Bestuurders gerechten

Portefeuillehouder gegevensbescherming is eindverantwoordelijk voor het hele gerecht.

Privacy coördinator

Is verantwoordelijk voor beleidsvorming en uitvoering beleid.

Privacy coördinator ondersteunt gerechtsbestuur en is intern adviseur.

Hoofden afdelingen en teams

Hoofden afdelingen en teams zijn eindverantwoordelijk voor het naleven van wet- en regelgeving binnen het team.

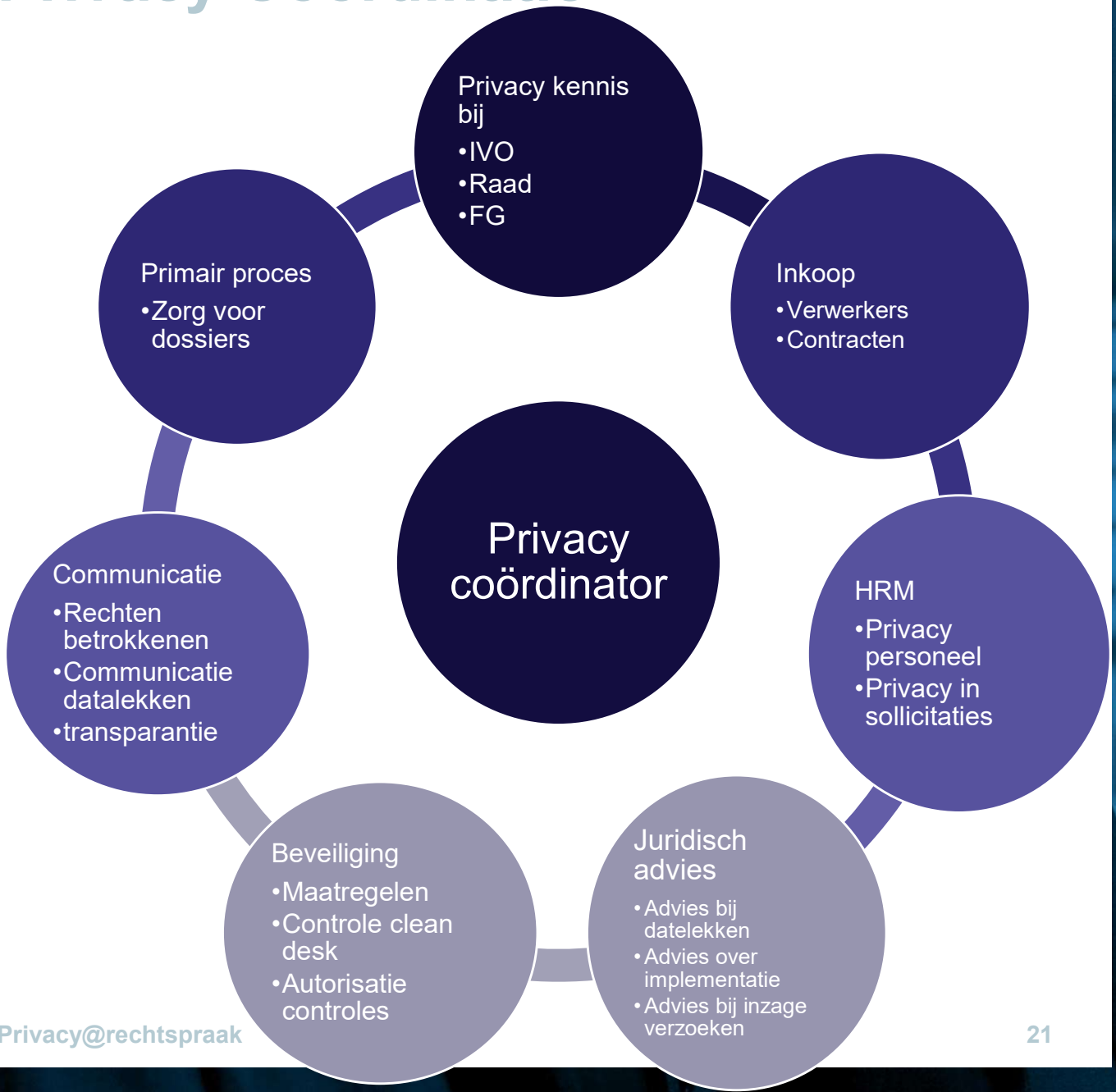
Contactpersonen afdelingen en teams

Fungeren als contactpersoon voor de privacy coördinator en als interne privacy champion en aanspreekpunt voor het team.

Privacy coördinatoren gerechten en diensten

- Ontwikkeling beleid en procedures;
- Intern adviseur voor afdelingen en teams;
- Stimuleren van bewustwording en kennisdeling;
- Uitvoeren meldprocedure datalekken;
- Ondersteunen bij lokale inventarisaties waaronder het aanwijzen van passende beheersmaatregelen
- Evalueren van aandachtspunten en zorgpunten en het opnemen van deze punten in een actieplan
- Monitoren en rapporteren over de uitvoering van het beleid en van actieplannen

Privacy Coördinatie



Advies lokale invoering privacy management

de Rechtspraak

Stap 1: Omschrijf taken, verantwoordelijkheden en bevoegdheden

Stap 2: Stel concreet en eenvoudig te begrijpen beleid op

Stap 3: Draag het beleid uit en blijf dit uitdragen (intro lokaal)

Stap 4: Evalueer regelmatig zorgen en aandachtspunten

Stap 5: Neem zorgen en aandachtspunten op in actieplan

Stap 6: Voer het actieplan uit

Stap 7: Neem structurele verbeteringen op in het (meer)jaarplan

Document 5:
20180522 Presentatie Implementatie AVG en Richtlijn - gegevensbescherming politie en justitie (Wjsg)

Implementatie AVG en Richtlijn gegevensbescherming politie en justitie (Wjsg)

Structurele bescherming van persoonsgegevens van betrokkenen in rechtszaken en van personele en overige gegevens

Bescherming persoonsgegevens

de Rechtspraak

AVG@Rechtspraak

Datum: 22 mei 2018

Programma

Programma

12.30 - 13.00	Inloop (zonder lunch)
13.00 - 14.00	Privacy governance en beleid
14.00- 14.30 uur	Pauze
14.30 – 15.30 uur	Interne bewustwording en communicatie (tips en trics)
15.30 – 16.00 uur	Vragen en afsluiting
16.00 - 17.00	Actieplannen en vervolgstappen

Vragen

- Waarom is privacy belangrijk voor de Rechtspraak?
- Kunnen de verwerkingen binnen de Rechtspraak gezien worden als verwerkingen met een hoog risico?
- Wat zijn de uitkomsten van de besluitvorming in het PRO?
- Wat is de stand van zaken met betrekking tot de implementatie?
- Zijn we in control én compliant voor 25 mei? Wat is het verschil?
- Wat moet er nog na 25 mei gebeuren?
- Hoe verloopt de procedure rechten betrokkenen?
- Verandert er nog iets in de procedure datalekken?
- Wanneer moet er nou een verwerkersovereenkomst afgesloten worden en wanneer niet?
- Hoe zit het met het privacybeleid HRM?
- Interne bewustwording en communicatie?

WAAROM IS PRIVACY BELANGRIJK VOOR DE RECHTSPRAAK?

Waarom is privacy belangrijk voor de rechtspraak?

1. Veel gevoelige en bijzondere gegevens
2. Communicatieve vrijheid in het rechtsproces
3. Vertrouwen in de Rechtspraak

De rechtspraak verwerkt veel gevoelige en bijzondere gegevens

de Rechtspraak

Gevoelige en bijzondere gegevens

De rechtspraak verwerkt veel gevoelige en bijzondere gegevens over:

- Relatie tussen privépersonen
- Relaties tussen werkgevers en werknemers
- Relaties tussen producten en consumenten
- Relaties tussen burgers en overheden
- Gegevens over vreemdelingen
- Medische, biometrische en genetische gegevens
- Strafrechtelijke gegevens
- Financiële en fiscale gegevens
- Enzovoorts.

De gegevens die de Rechtspraak verwerkt worden in de AVG en de Richtlijn gezien als gegevens met een **hoog risicoprofiel**.

Communicatieve vrijheid in het rechtsproces

de Rechtspraak

Ongestoorde uitwisseling van informatie en standpunten

Privacy stelt mensen in staat zich vrijelijk te kunnen uiten in de wetenschap dat informatie vertrouwelijk blijft.

Rechtszoekenden moeten informatie kunnen delen met de rechter zonder druk.

Het zou het rechtsproces geen goed doen als mensen informatie niet meer durven delen met de rechter uit vrees dat informatie wordt misbruikt, in verkeerde handen komt of (te) openbaar wordt.

Privacy vormt zo een van de basisvoorwaarden voor een eerlijk rechtsproces.

Trias politica: wetgeving, rechtspraak en uitvoering

Gezonde balans tussen privacy, controle en openbaarheid is cruciaal.

Vertrouwen in de rechtspraak

de Rechtspraak

Vertrouwen in het recht en de rechtsbescherming

- De Rechtspraak heeft een voorbeeldfunctie
- Als wij het al niet goed doen, wie dan wel?

Vertrouwen van burgers

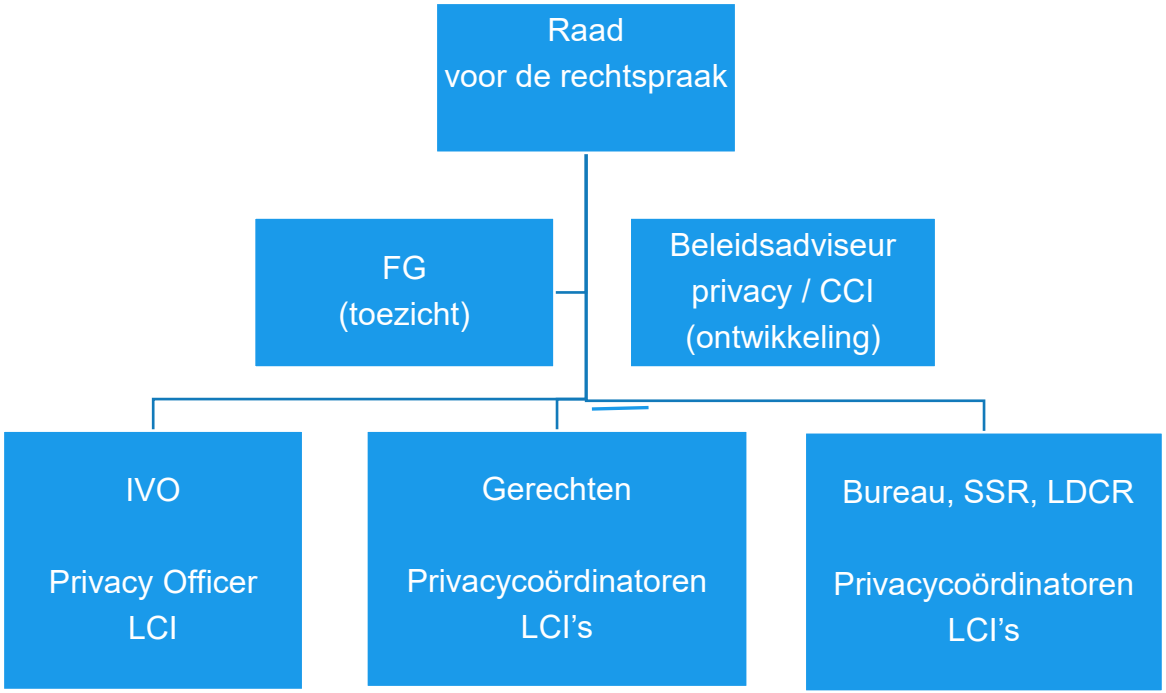
- Burgers vertrouwen ons informatie toe
- Burgers vertrouwen dat de rechtspraak privacy beschermt

Vertrouwen van ketenpartijen en professionele partijen

- De Rechtspraak vormt een knooppunt van informatiestromen.
- Onrechtmatige verwerking of datalekken heeft ook impact op ketenpartijen en professionele partijen.

HOE IS DE GOVERNANCE GEORGANISEERD?

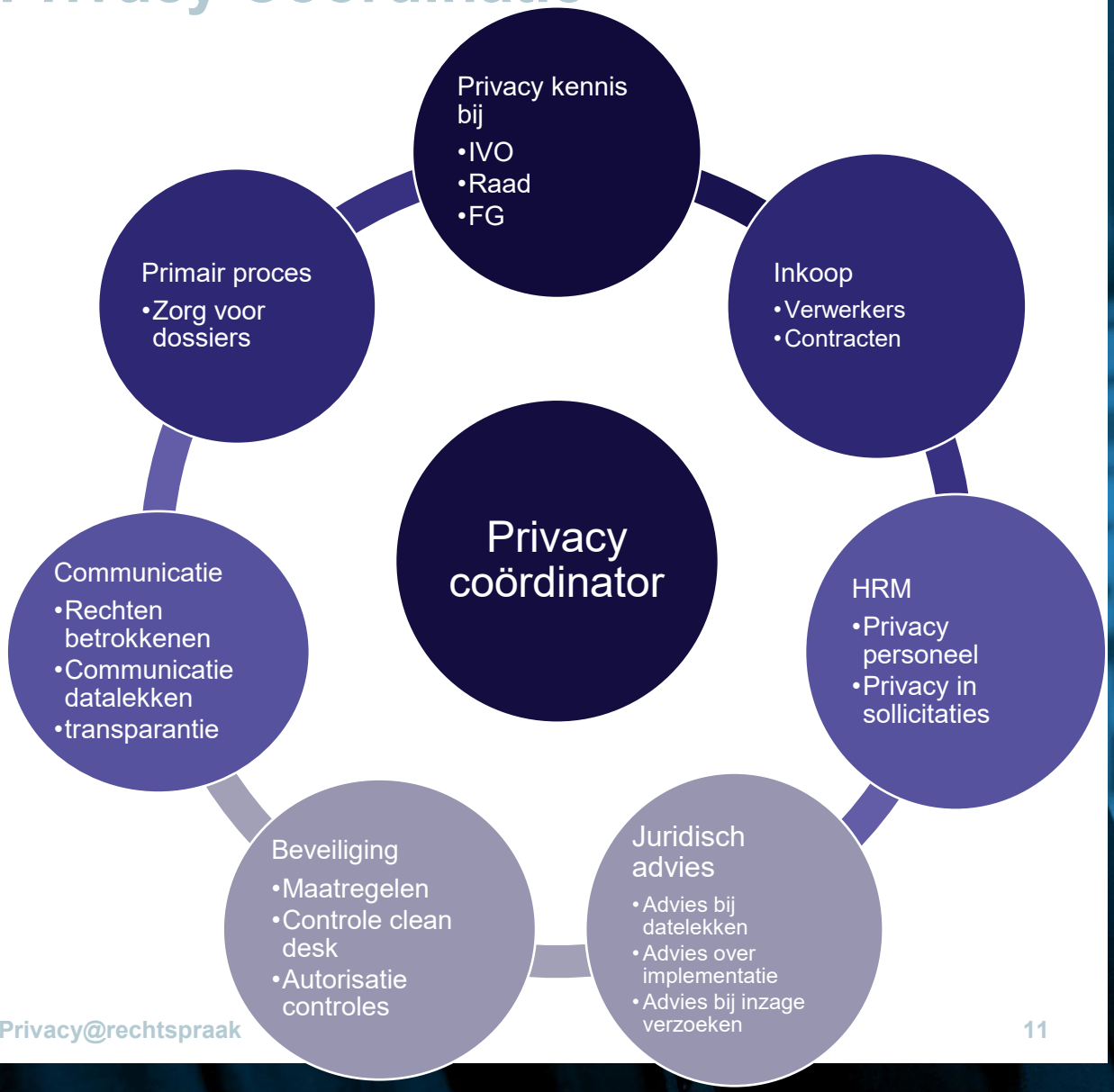
Governance



CCI: Centraal coördinator informatieverzoeken
LCI: Lokaal coördinator informatieverzoeken

Iedere organisatie: portefeuillehouder/ eindverantw.

Privacy Coördinatie



Algemeen privacybeleid

- Privacy governance
- Privacybeleid
- Beveiligingsbeleid
- Register van verwerkingen
- Privacy Impact Assessment
- Privacy by design / default
- Datalekken
- Rechten betrokkenen
- Verwerkersovereenkomsten
- Functionaris gegevensbescherming
- Samenwerken met toezichthoudende autoriteiten
- Gedragscodes of certificering

Specifiek privacybeleid

- Verzameling en registratie;
- Bewaren en archiveren;
- Autoriseren;
- Uitwisseling gegevens met procespartijen, ketenpartijen, professionele partijen en derden;
- Wetenschappelijk, statistisch en historisch onderzoek;
- Doorgiften aan derde landen of organisaties;
- Persrichtlijnen;
- Publicatie van registers en uitspraken;
- Openbaarheid van bestuur;
- Nieuwsbrieven;
- Websites en cookie;
- Big data en open data;
- Postverwerking;
- Vernietiging gegevensdragers (papier en digitaal).

Extern Toezicht

de Rechtspraak

AVG artikel 55, lid 3

Toezichthoudende autoriteiten zijn niet competent toe te zien op verwerkingen door gerechten bij de uitoefening van hun rechtsprekende taken.

Overweging 20

De competentie van de toezichthoudende autoriteiten mag zich niet uitstrekken tot de verwerking van persoonsgegevens door gerechten in het kader van hun gerechtelijke taken, zulks teneinde de onafhankelijkheid van de rechterlijke macht bij de uitoefening van haar rechterlijke taken, waaronder besluitvorming, te waarborgen. Het toezicht op die gegevensverwerkingen moet kunnen worden toevertrouwd aan specifieke instanties binnen de rechterlijke organisatie van de lidstaat, die met name de naleving van de regels van deze verordening moeten garanderen, leden van de rechterlijke macht van hun verplichtingen krachtens deze verordening sterker bewust moeten maken, en klachten met betrekking tot die gegevensverwerkingen moeten behandelen.

Hoe wordt dit dan georganiseerd?

Zie voor meer informatie: www.rechtspraak.nl/privacy

(hoe kan ik een klacht indienen?)

EVALUATIE EN BIJSTELLING GOVERNANCE (NOVEMBER 2018)

- Hoe staat het er nu voor?
- Actiepunten van het landelijk actieplan?
- Ervaringen van de afgelopen maanden?
- Is er voldoende capaciteit om privacy management structureel te borgen?
- Zijn de functies goed verdeeld?

STAND VAN ZAKEN

BLIK NAAR DE TOEKOMST

Stand van zaken algemeen

Onderdeel	Gereed	Toelichting
Register van verwerkingen		155 applicaties honderden lijsten
Governance		FG, Privacy Officer IVO, coördinatoren.
Algemeen privacybeleid		Gereed
Privacyverklaring		Gereed
Rechtspraak.nl		Gereed
In-control (overzicht / inzicht)		Gereed
Specifiek privacybeleid		Verder uitwerken
Interne bewustwording		Going concern
Administratie/interne controle		Opzet in concept
Compliancy		1 januari 2019
Structurele borging		Moet blijken, daarom eind 2018: evaluatie.

Beleid en procedures

Procedures en regels	Gereed	Toelichting
Datalekken		Loopt al een tijd
Privacy Impact Assessment		Loopt al een tijd
Rechten betrokkenen		Basis redelijk tot goed
Overzicht privacyregels		Verder uitwerken
Best practices HRM		Nog afstemmen COR
Beleid privacy by design		Wordt ingevoerd
Externe uitwisseling (keten)		Basisoverzicht op orde

Aanpassen processen en systemen → compliancy

Procedures en regels	Gereed	Toelichting
Gedrag (volgen privacyregels)		Structurele borging en bewustwording
Systemen (privacy by design)		Aanpassen systemen, meerjarenplan
Verwerkersovereenkomsten		Tot 1 januari 2019
Schonen archieven		Achterstanden, meerjarenplan
Autorisaties / bevragingen		Toegang beperken

Nazorg tot 1 januari 2019

de Rechtspraak

Eindrapportage project implementatie AVG en Richtlijn
Eind juni gereed, inclusief landelijk plan van acties.

Autorisaties en bevragingen
Gerechten dienen dit op orde te brengen.

Systeemaanpassingen (backlog)
Privacy by design structureel doorvoeren bij IVO

Best practices HRM
Is besproken in vakgroep HRM.

Vakinhoudelijke opleidingen in privacyrecht
Themadag SSR over Privacy op 28 september 2018

Evaluatie en bijstelling in november 2018
Governance en beleid evalueren

Strategische keuzes na 1 januari 2019

de Rechtspraak

IT ontwikkeling en beheer (visie op functie IT applicaties)

Structureel doorvoeren privacy impact assessment
Privacy by design op een hoger plan
Gegevensgericht autorisaties

Uitwisseling van gegevens (ketenvisie)

Delen van informatie tussen procespartijen
Delen van informatie met ketenpartijen en professionele partijen
Big Data, Open Data, Openbaarheid

Rechtspraakarchieven

Wegwerken achterstanden
Digitalisering van archieven
Privacy in digitale archieven
Uitdagingen: wetenschappelijk onderzoek.

Wat komt er nog op Intro Landelijk en Rechtspraak.nl?

- Best Practices HRM
- Handreiking privacyregels Rechtspraak (antwoord op alle vragen)
- Procedure rechten betrokkenen + modelbrieven
- Nieuwe procedure verwerkersovereenkomsten
- Publicatie privacyverklaring en extern register op Rechtspraak.nl

Procedure rechten betrokkenen (themamiddag 07 mei)

Ontvangst verzoek

Gerecht of Raad voor de rechtspraak

Brief bevestiging ontvangst + eventueel preciseringsverzoek

Betrokkene wordt mede gedeeld dat aan hem of haar gevraagd kan worden om zich te komen identificeren

Verzamelen van informatie

Interne afstemming

Brief met uitnodiging om zich te komen legitimeren

Afhandeling verzoek: twee opties:

1. Betrokkene ontvangt informatie of bevestiging van correctie direct
2. Betrokkene ontvangt kort daarop per post de gevraagd informatie

DEEL 2
COMMUNICATIE, BEWUSTWORDING EDUCATIE
IN DE PRAKTIJK

INTERNE BEWUSTWORDING BINNEN DE EIGEN ORGANISATIE

- **Geven van presentaties**
  - Teams/afdelingen informeren over grondslagen AVG/Richtlijn
  - lokale presentaties voor inkoop, communicatie, etc.
  - Standaardpresentaties via Intro Landelijk

- **Berichten op Intro Lokaal**
  - attenderen op aandachtspunten en risico's

- **Workshops over verschillende onderwerpen:**
  - Veilig versturen van gegevens

- **Dialoog**
- - Dialoog over verwerking persoonsgegevens primair proces

- **Bevindingen en zorgen in actieplannen**
- Bevindingen en zorgen opnemen in actieplannen

- **Pro memorie: gedragscode privacy**

Kennisdeling

- **Informatievoorziening privacypagina**
- **- Meer informatie opnemen op privacypagina.**
- **- Standaardpresentaties, factsheets, etc.**

- **Wikipagina**
- **- Kennis delen via Wiki-pagina**
- **- voor de vakinhoud is er al een Wiki-pagina AVG/Richtlijn**

- **Teamsite privacy coördinatoren en LCI's**
- **- wordt in juni opgezet**

- **Lijst met interessate sprekers die presentaties kunnen geven**
- **- Projectteam: lijst is in de maak**

Waar zou “jij bent de sleutel” aandacht kunnen vragen?

- **Versturen van gegevens via veilige Rechtspraakkanalen**
- **Versturen processtukken via e-mail mag niet, wat zijn alternatieven?**

- **Rechtmatigheid verstrekkingen**
- **Dillema’s benoemen en adresseren**

- **Bewaren gegevens**
- **Hoe lang gegevens bewaren in mailbox of mappen?**

- **Toegang tot gegevens**
- **Toegang tot zaaksdossiers, vertrouwelijk behandelen van documenten**

- **Datalekken**
- **Meer aandacht voor wat en datalek is en wat te doen.**

Landelijk Overleg of werkgroep?

- Landelijk Privacy Overleg (LPO)
- Landelijk Overleg Gegevensbescherming (LOG)
- Privacy Overleg (PRIVO)
- Rechtspraak Privacy Overleg (RPO)
- Privacy Overleg Rechtspraak (POR)
- Privacy Overleg Rechtelijke Organisatie (PORO)
- Werkgroep Gegevensbescherming Rechtspraak (WGR)

Hierover zijn we nog niet uit ☺. Als iemand ideeën heeft dan horen we die graag.

Educatie

Soorten

- Opleidingen AVG en archieven
- Opleidingen AVG en HRM
- Opleidingen privacyrecht
- Opleidingen IT Privacy by design

Certificatie

- Certified Informatie Privacy Manager (CIPM) management
- Certified Information Privacy Technologist (CIPT) ICT
- Certified Information Privacy Practitioner (CIPP) recht

Opleidingsinstituten en type opleidingen:

- Projectteam: overzicht is in de maak

Document 6:
20180525 Handreiking verwerkersovereenkomsten (ten behoeve van inkoop)

Handreiking verwerkersovereenkomsten (ten behoeve van inkoop)

Inleiding

Bij de verwerking van persoonsgegevens maakt de Rechtspraak in sommige gevallen gebruik van diensten van derde partijen. De uitvoering van verwerkingen van persoonsgegevens door een derde partij moet geregeld worden in een overeenkomst. Dit kan in een samenwerkingsovereenkomst, of in een apart document, de verwerkersovereenkomst. De punten zoals deze in de verwerkersovereenkomst zijn opgenomen moeten schriftelijk of in elektronische vorm zijn vastgelegd. U leest in dit factsheet alles over de wettelijke verplichtingen ten aanzien van de afspraken. Dit factsheet biedt houvast bij het bepalen of een verwerkersovereenkomst verplicht is en wat er vervolgens in de overeenkomst moet zijn opgenomen. Ook in gevallen waarin een verwerkersovereenkomst niet wettelijk verplicht is, loont het de moeite om afspraken te maken met leveranciers en derde partijen over de omgang met persoonsgegevens en de verdeling van wettelijke taken.

Leeswijzer

De handreiking is als volgt opgebouwd:

1. Algemene begrippen

AVG en de Richtlijn

Iedereen heeft recht op bescherming van zijn of haar persoonsgegevens (art. 10 lid 1 van de grondwet, art. 8 Handvest van de grondrechten van de EU, en art. 16 lid 1 Verdrag betreffende de werking van de Europese Unie (VWEU)). Deze bescherming is vastgelegd in de algemene verordening gegevensbescherming (AVG, (EU) 2016/679) Dat betekent dat er vanaf die datum nog maar één privacywet geldt in de hele Europese Unie (EU) . In het licht van de toenemende digitalisering en de juridische wijzigingen zijn publieke organisaties actief aan de slag om in hun dienstverlening de privacy van alle betrokkenen te waarborgen. Deze waarborgen moeten niet alleen intern in de eigen organisatie worden aangebracht, maar zeker ook in dienstverleningen uitgevoerd door derden.

Hoewel de AVG niet van toepassing is op justitiële en strafvorderlijke gegevens, hiervoor richtlijn 2016/680. van toepassing, zijn de eisen die in de richtlijn worden gesteld rondom de verwerkers en de contracten hiermee gelijken aan de eisen in de AVG. In dit document zal dus geen onderscheid worden gemaakt tussen de AVG en de Richtlijn.

Verantwoordelijke en verwerker

Overheden en daarmee vergelijkbare organisaties hebben steeds vaker (een deel van) hun persoonsgegevens ondergebracht bij externe leveranciers en maken gebruik van derden die in opdracht persoonsgegevens verwerkt. Deze derde partijen kwalificeren veelal als verwerker, de overheidspartijen zelf zijn verwerkingsverantwoordelijk.

Verwerkingsverantwoordelijke:

een natuurlijke- of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht

worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Wettelijke verplichtingen
Uit de wet volgt dat elke handeling (verwerking of bewerking) met betrekking tot persoonsgegevens (alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon) aan bepaalde eisen is gebonden.

Verwerkersovereenkomst
De uitvoering van verwerkingen door een verwerker dient geregeld te worden in een overeenkomst, of in een wettelijke regeling tussen een verwerkingsverantwoordelijke en een verwerker. Bindende afspraken tussen de verwerkingsverantwoordelijke en verwerker kunnen ook blijken uit andere rechtshandelingen, mits voldaan wordt aan de vereisten. Volgens de AVG kunnen de verwerkingsverantwoordelijke en verwerker in plaats van een individuele verwerkersovereenkomst ook 'standaardcontractbepalingen' gebruiken.
De verwerkersovereenkomst geeft de keten in het proces van verwerking tussen de verwerkingsverantwoordelijke, verwerkers en subverwerkers weer en geeft inzicht in de verdeling van verantwoordelijkheden en aansprakelijkheden. De overeenkomst geeft tenminste inzicht in onderwerp en duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en categorieën van betrokkenen, de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.
Het is van belang met leveranciers minimaal afspraken te maken over de volgende wettelijke verplichtingen:

- De waarborgen die de leverancier biedt ten aanzien van technische en organisatorische maatregelen en de manier waarop dit gecontroleerd kan worden;
- De wijze waarop de opdrachtgever wordt geïnformeerd bij een beveiligingsincident en welke administratie de leverancier bijhoudt;
- De aansprakelijkheid bij schade doordat in strijd met de wet wordt gehandeld door de leverancier.

De kern is dat de verwerkingsverantwoordelijke verantwoordelijk en aansprakelijk is en blijft voor de gegevensverwerking, de verwerker alleen gegevens verwerkt op basis van de schriftelijke instructie, en de verwerker de maatregelen zoals deze voorvloeien uit de overeenkomst met betrekking tot de bescherming van de persoonsgegevens uitvoert. Bij het inschakelen van verwerkers door de verwerkingsverantwoordelijke is het belangrijkste uitgangspunt dat deze verwerkers voldoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten voldoen en de bescherming van de rechten van de betrokkene is gewaarborgd .

Verwerkingsregister
Verwerkingsverantwoordelijke en verwerkers moeten een administratie (register) bijhouden, waarin alle activiteiten worden omschreven waarbij persoonsgegevens worden verwerkt, van alle verwerkingen, inclusief contactgegevens, het doel, de juridische grondslag, categorieën van betrokkenen, de persoonsgegevens, de ontvangers van de persoonsgegevens, een beschrijving van de beveiligingsmaatregelen en de beoogde bewaartermijnen, om de accountability te vergroten. Op verzoek van de toezichthouder, de Autoriteit Persoonsgegevens (AP) , dient de administratie aan de toezichthouder (AP) overhandigd te worden ter controle. Deze administratie is verplicht voor alle verwerkingsverantwoordelijke en verwerkers van persoonsgegevens. Het door de verwerkingsverantwoordelijke in te richten register bevat ook (daar waar van toepassing) verwijzingen naar verwekkers.

Meldplicht datalekken
De AVG kent een meldplicht datalekken, de term in de AVG is 'een inbreuk in verband met persoonsgegevens' in plaats van datalek. Op het moment dat er per ongeluk, of opzettelijk, data verloren gaan, of er een mogelijke

onterecht openbaring is van persoonsgegevens (persoonsgegevens zijn mogelijk ingezien door een daartoe niet bevoegde), moet dit binnen 72 uur aan de externe toezichthouder (AP), en wanneer die inbreuk in verband met persoonsgegevens grote risico's voor de rechten en vrijheden van de natuurlijke persoon met zich kan brengen ook aan de betrokkene zelf.
De AVG kent grote administratieplicht . De verwerkingsverantwoordelijke administreert 'alle inbreuken', dus ook de niet extern meldingsplichtige. De verwerker heeft de plicht om de verwerkingsverantwoordelijke zonder onredelijke vertraging te informeren over een mogelijke inbreuk binnen de verwerking. De verwerker is zelf verantwoordelijk voor het uitvoeren van de documentatieplichten.

Subverwerkers alleen met toestemming
Verwerkers mogen geen subverwerker aanstellen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke.

Model verwerkersovereenkomst
De modellen verwerkingsovereenkomsten behorende bij de Algemene Rijksvoorwaarden [1]bij IT-overeenkomsten (ARBIT) en de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten (ARVODI) gaan over de verhouding tussen partijen en de in dat kader (al dan niet aanvullend) te maken afspraken. Leverancier neemt de rol van verwerker in. De modellen zijn in dit kader te beschouwen als (basis)verwerkersovereenkomst. Daar waar de afspraken uit deze modellen niet volstaan, kunnen een aanvullende of afwijkende verwerkersovereenkomst worden gesloten. Hiervoor is een model verwerkersovereenkomst beschikbaar gesteld.

2. Toepassing binnen de Rechtspraak

Inleiding
De Rechtspraak heeft als streven op opdrachten voor de verwerking van persoonsgegevens door derden die geen onderdeel uitmaken van de rechtspersoon Staat der Nederlanden de ARBIT of de ARVODI van toepassing te verklaren. Dat zijn Rijksbrede opgestelde modelovereenkomsten met bijbehorende algemene voorwaarden. Met het oog op de AVG zijn ook de bijbehorende verwerkersoverkomsten aangepast (onder de Wbp spraken we van bewerkersovereenkomsten).

ARVODI:
[redacted]

ARBIT:
[redacted]

Deze modelverwerkersovereenkomsten gelden dus als overeenkomsten conform de ARBIT en de ARVODI zijn afgesloten. Worden er overeenkomsten afgesloten op basis van een andere overeenkomst, dan dienen de modellen dus aangepast te worden. Uiteraard kan er wel veel input gebruikt worden uit deze modellen.

[1] https://zoek.officielebekendmakingen.nl/stcrt-2016-51478.html

Verwerkersprotocol met onderdelen Staat
Ministeries en overige onderdelen van de Staat der Nederlanden hebben onderling afgesproken geen verwerkersovereenkomsten met elkaar af te sluiten maar in plaats daarvan kan een verwerkersprotocol worden afgesloten.
Als Rechtspraak hebben we besloten – wegens de onafhankelijke positie – altijd zo'n verwerkersprotocol af te sluiten met onderdelen die binnen de Staat der Nederlanden vallen. Er hoeft dus geen model verwerkersprotocol binnen de Rechtspraak te worden opgesteld. Dit verwerkersprotocol bestond dus onder de Wbp nog niet en is dus speciaal voor de AVG opgesteld.

Vanuit het Rijk is nog een handige checklist opgesteld:
[redacted]

Overeenkomsten van vóór 25 mei en van na 25 mei
Tot slot nog nadere uitleg wat te doen met overeenkomsten van vóór 25 mei en van na 25 mei. Hierover staat ook diverse informatie op het Rijksportaal (zie ook de bovenstaande linken).

Informatie Rijksportaal:

<u>Nieuwe overeenkomsten vanaf 25 mei 2018:</u>
Vanaf 25 mei 2018 kunnen de model verwerkersovereenkomsten gewoon worden toegevoegd aan eventuele nieuwe overeenkomsten die worden afgesloten op basis van de ARBIT en de ARVODI. Aanpassing van de ARBIT en de ARVODI is namelijk op die datum voorzien, zodat de model verwerkersovereenkomsten daar geheel naadloos op aan sluiten.

<u>Opdrachten vanaf nu tot 25 mei 2018:</u>
Voor opdrachten die in de aanloop naar 25 mei 2018 zijn of worden gesloten op basis van de ARBIT-2014 en de ARVODI-2014 of de ARBIT-2016 en de ARVODI-2016, dienen er twee extra bepalingen te worden opgenomen in de hoofdovereenkomst. Dat betekent dus dat er gebruik gemaakt dient te worden van het nieuwe model verwerkersovereenkomst en dat er twee bepalingen toegevoegd dienen te worden aan de hoofdovereenkomst. Het gaat om artikelen over de bescherming van persoonsgegevens en aansprakelijkheid. Ter info zijn ze hieronder opgenomen:

ARBIT-2016
Indien er sprake is van de verwerking van persoonsgegevens en er een Verwerkersovereenkomst wordt gesloten, moeten in de Modelovereenkomst onder kopje 10 'Overige bepalingen' de volgende artikelen worden opgenomen:

- In aanvulling op artikel 26.4 ARBIT-2016 komen de in de artikelen 26.2 en 26.3 ARBIT-2016 opgenomen beperkingen van aansprakelijkheid ook te vervallen ten aanzien van aanspraken op schadevergoeding, waaronder mede begrepen de door de toezichthoudende autoriteit opgelegde boetes, in verband met tekortschieten in de nakoming van de Verwerkersovereenkomst.
- Artikel 18 van de ARBIT-2016 is niet van toepassing.

ARVODI-2016
Indien er sprake is van de verwerking van persoonsgegevens en er een Verwerkersovereenkomst wordt gesloten, moeten in de Dienstverleningsovereenkomst onder kopje 6 'Overige Voorwaarden' de volgende artikelen worden opgenomen:

- In aanvulling op de in artikel 21.3 van de ARVODI-2016 opgenomen afwijking van de beperking van aansprakelijkheid vervalt deze beperking van de aansprakelijkheid ook ten aanzien van aanspraken op

schadevergoeding, waaronder mede begrepen de door de toezichthoudende autoriteit opgelegde boetes, in verband met tekortschieten in de nakoming van de Verwerkersovereenkomst.
- Artikel 14 van de ARVODI-2016 is niet van toepassing.

Afhankelijk van de aard van de opdracht moeten deze artikelen worden toegevoegd aan de Modelovereenkomst, de Raamovereenkomst of de Nadere overeenkomst.

Huidig afgesloten bewerkersovereenkomsten op basis van de ARBIT-2014 en de ARVODI-2014 of de ARBIT-2016 en de ARVODI-2016

Lopende overeenkomsten op basis van een bewerkersovereenkomst moeten worden aangepast als de expiratiedatum **na 25 mei 2018 ligt**. Het advies Rijksbreed is de bewerkersovereenkomst te vervangen door een nieuw model verwerkersovereenkomst en de twee artikelen zoals hiervoor genoemd toe te voegen aan de hoofdovereenkomst.
Tot slot is nog bedoeld dat deze modelovereenkomsten bedoeld zijn voor AVG-verwerkingen. Er wordt Rijksbreed nog onderzocht of er een specifiek model moet worden opgesteld voor verwerkingsactiviteiten die zijn gebaseerd op de Richtlijn voor de politiegegevens en strafrechtelijke gegevens.

Register van verwerkersovereenkomsten

Binnen de Rechtspraak beginnen we met het maken van een overzicht van alle leveranciers die in opdracht van onze organisatie diensten verlenen die betrekking hebben op de verwerking van persoonsgegevens. Vervolgens kan worden nagegaan of met alle leveranciers afspraken zijn gemaakt en of deze aangepast moeten worden naar de regels van de AVG. Onderstaand treft u de twee belangrijkste uitgangspunten als leverancier en onze organisatie met elkaar in overleg gaan over de verwerkersovereenkomst:

3. Inhoud verwerkersovereenkomst

De inhoud van een verwerkersovereenkomst moet minimaal de volgende vier punten omvatten;

- onderwerp en duur van de verwerking,
- de aard en het doel van de verwerking,
- het soort persoonsgegevens en categorieën van betrokkenen,
- de rechten en verplichtingen van de verwerkingsverantwoordelijke

Hiernaast moet een verwerkersovereenkomst de volgende verplichtingen opleggen aan de verwerker;

- de persoonsgegevens uitsluitend te verwerken op basis van de schriftelijke instructies van de verwerkingsverantwoordelijke;
- de vertrouwelijkheid in acht te nemen;
- passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen;
- bijstand te verlenen als de betrokkene een van zijn rechten uitoefent;
- na afloop van de verwerkingsdiensten, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert;
- medewerking te verlenen bij audits;
- de verwerkingsverantwoordelijke zonder onredelijke vertraging te informeren zodra de verwerker kennis heeft genomen van een inbreuk in verband met persoonsgegevens;
- alleen subverwerkers aanstellen na schriftelijke toestemming van de verantwoordelijke en met een eventuele subverwerker dezelfde afspraken te maken als die gelden tussen de verwerkingsverantwoordelijke en de verwerker.

Omschrijving van de persoonsgegevens / onderwerp van de overeenkomst
In het eerste gedeelte van de verwerkersovereenkomst dient een omschrijving van de inhoud, de duur van de verwerking te worden opgenomen. Beide zullen in de meeste gevallen gelijk zijn aan de overeenkomst (het contract) tussen de verwerker en de rechtspraak. Hiernaast moet de aard en het doel van de verwerking, de soorten persoonsgegevens en categorieën van betrokkenen te worden opgenomen. Deze gegevens zullen in de regel ook in het verwerkingsregister zijn opgenomen. Tevens omschrijft dit gedeelte ook de rechten en plichten van de verwerkingsverantwoordelijke ten aanzien van de verwerker. Hieronder vallen bijvoorbeeld het recht op controle (audit) van de verwerking.

Dienstverlening
De verwerkersovereenkomst moet beschrijven welke diensten de verwerker verleent met betrekking tot de persoonsgegevens (voor de verwerkingsverantwoordelijke). De verwerking moet in overeenstemming zijn met instructies van de verwerkingsverantwoordelijke. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verwerkingsverantwoordelijke. Er zullen afspraken gemaakt moeten worden omtrent de geheimhouding van de persoonsgegevens en over de geheimhouding door de personen die ten behoeve van de diensten werken met deze persoonsgegevens.

Betrouwbaarheidseisen
Persoonsgegevens kunnen onder verschillende categorieën worden onderverdeeld. Voor ieder van de verschillende categorieën dienen afspraken vastgelegd te worden in de verwerkersovereenkomst.

Beveiliging en continuïteit
In de verwerkersovereenkomst moeten afspraken worden gemaakt betreffende de (technische en organisatorische) beveiliging van de persoonsgegevens om zorg te dragen voor de vertrouwelijkheid, integriteit en beschikbaarheid van de persoonsgegevens. De verwerkingsverantwoordelijke draagt zorg dat de verwerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen tegen verlies et cetera. De afspraken mogen niet algemeen zijn en moeten gedetailleerd worden vastgelegd. Deze afspraken moeten beantwoorden aan de voorschriften uit de regeling en de AVG met betrekking tot maatregelen en beveiliging van de gegevens.

Transparantie over de beveiliging
De verwerker en de verwerkingsverantwoordelijke moeten ook afspraken maken over de rapportages over de beveiliging. In de verwerkersovereenkomst dienen de inhoud en de frequentie van de rapportages te worden vastgelegd. Ook moet de verwerkingsverantwoordelijke het recht hebben om de gehanteerde beveiligingseisen door de verwerker door een deskundige te laten inspecteren.

Transparantie over beveiligingsincidenten en datalekken
Transparantie gaat over de inhoud van de rapportages van beveiligingsincidenten en de snelheid waarmee moet worden gerapporteerd. Als zich een beveiligingsincident heeft voorgedaan is het belangrijk dat er wordt gerapporteerd aan de verwerkingsverantwoordelijke en – eventueel – de betrokkenen. In de afspraken moet worden opgenomen dat en op welke wijze de verwerker beveiligingsincidenten en datalekken die (mogelijk) gevolgen hebben voor betrokkenen meteen rapporteert aan de verwerkingsverantwoordelijke. Tevens moet worden vastgelegd dat de verwerker bij een beveiligingsincident waar nodig meewerkt aan het adequaat informeren van betrokkenen.

Verwerking van persoonsgegevens buiten Nederland/EU
Een ander belangrijk onderdeel van de verwerkersovereenkomst gaat over afspraken over welke persoonsgegevens in welke landen worden verwerkt (met name van belang: opgeslagen) en onder welke voorwaarden. Let op: wanneer persoonsgegevens buiten de EU worden verwerkt zijn extra waarborgen voor

de verwerking van de persoonsgegevens vereist. Het doorgeven van persoonsgegevens buiten de EU mag alleen wanneer dit land of de organisatie voldoende bescherming biedt.

Locatie van de data
De verwerkingsverantwoordelijke moet weten in welke landen zijn data worden opgeslagen. Dit is mede van belang met het oog op de verplichtingen die gelden bij doorgifte van persoonsgegevens naar het buitenland. Het is noodzakelijk om hierover afspraken te maken en deze vast te leggen in de verwerkingsovereenkomst.

Verwerking door subverwerkers
In de verwerkersovereenkomst wordt vastgelegd of de verwerker met voorafgaande toestemming subverwerkers inschakeld. De subverwerkers moeten door de verwerker minimaal aan de zelfde vereisten voldoen als de verwerker zelf. Een Verwerker mag geen subverwerker aan stellen voor de verwerking zonder voorafgaande toestemming van de verwerkingsverantwoordelijke.

Verzoeken van betrokkenen
In de verwerkersovereenkomst dienen afspraken te worden gemaakt over de wijze waarop de verwerker zijn medewerking dient te verlenen aan verzoeken van betrokkenen om inzage , verbetering, aanvulling, verwijdering en afscherming van persoonsgegevens waar de verwerker toegang tot heeft.

Aansprakelijkheid
De wet bepaalt dat de verwerkingsverantwoordelijke kan worden aangesproken als iemand schade lijdt doordat de wet niet wordt nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de verwerker, die in dat geval ook zelfstandig aansprakelijk is. De aansprakelijkheidsverdeling van verwerkingsverantwoordelijke en verwerker voor de schade voortvloeiende uit het niet nakomen van de afspraken die zijn vastgelegd in de verwerkersovereenkomst moet worden geregeld.

Controle en audits
Er dienen afspraken te worden gemaakt over de mogelijkheid voor de verwerkingsverantwoordelijke om te kunnen controleren of de verwerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verwerkingsverantwoordelijke of door een onafhankelijke derde. In de verwerkersovereenkomst moeten de mogelijkheden over het uitvoeren van audits worden vastgelegd. Verder dient in de verwerkersovereenkomst aandacht te worden besteed aan de rangorde van overeenkomsten tussen verwerkingsverantwoordelijke en verwerker en het toepasselijk recht.

Wijzigen of beëindigen van de verwerkersovereenkomst
In de verwerkersovereenkomst moeten afspraken worden opgenomen over het wijzigen of beëindiging van de verwerkersovereenkomst. Ook een noodplan voor het geval één van de partijen de verwerkersovereenkomst wil beëindigen dient opgenomen te worden. Verder wordt hierin vastgelegd hoe de verwerkingsverantwoordelijke, na beëindiging van de dienstverlening door verwerker, de verwerkte persoonsgegevens weer ter beschikking krijgt. Ook moet er worden vastgelegd hoe wordt gewaarborgd dat de verwerker na het beëindigen van de verwerkersovereenkomst niet meer over de persoonsgegevens kan beschikken.

Bewaartermijnen, back-up en vernietiging
Omdat een verwerking een gehele levenscyclus van gegevens omvat (van collectie tot aan vernietiging) moeten in een verwerkersovereenkomst ook artikelen worden omtrent de bewaartermijnen, reservekopieën en vernietiging van de persoonsgegevens (bij beëindiging van de verwerkersovereenkomst).

Bijlage A: Beslisboom verwerkersovereenkomst

Wanneer de Rechtspraak persoonsgegevens laat verwerken door andere partijen, dan kan het nodig zijn om hierover afspraken te maken en deze vast te leggen in een zogenoemde verwerkersovereenkomst. De beslisboom (pagina 2) laat zien of een verwerkersovereenkomst nodig is. Als uit de beslisboom blijkt dat een verwerkersovereenkomst niet nodig is, maar de partijen wel persoonsgegevens verwerken, dan moet de Rechtspraak een veilige omgang met gegevens in andere afspraken opnemen. Welke afspraken (in overeenkomsten) dit zijn, staan in de beslisboom en toelichtingen vermeld.

Een aantal gebruikte termen in de beslisboom en in de toelichtingen, verdienen een toelichting:

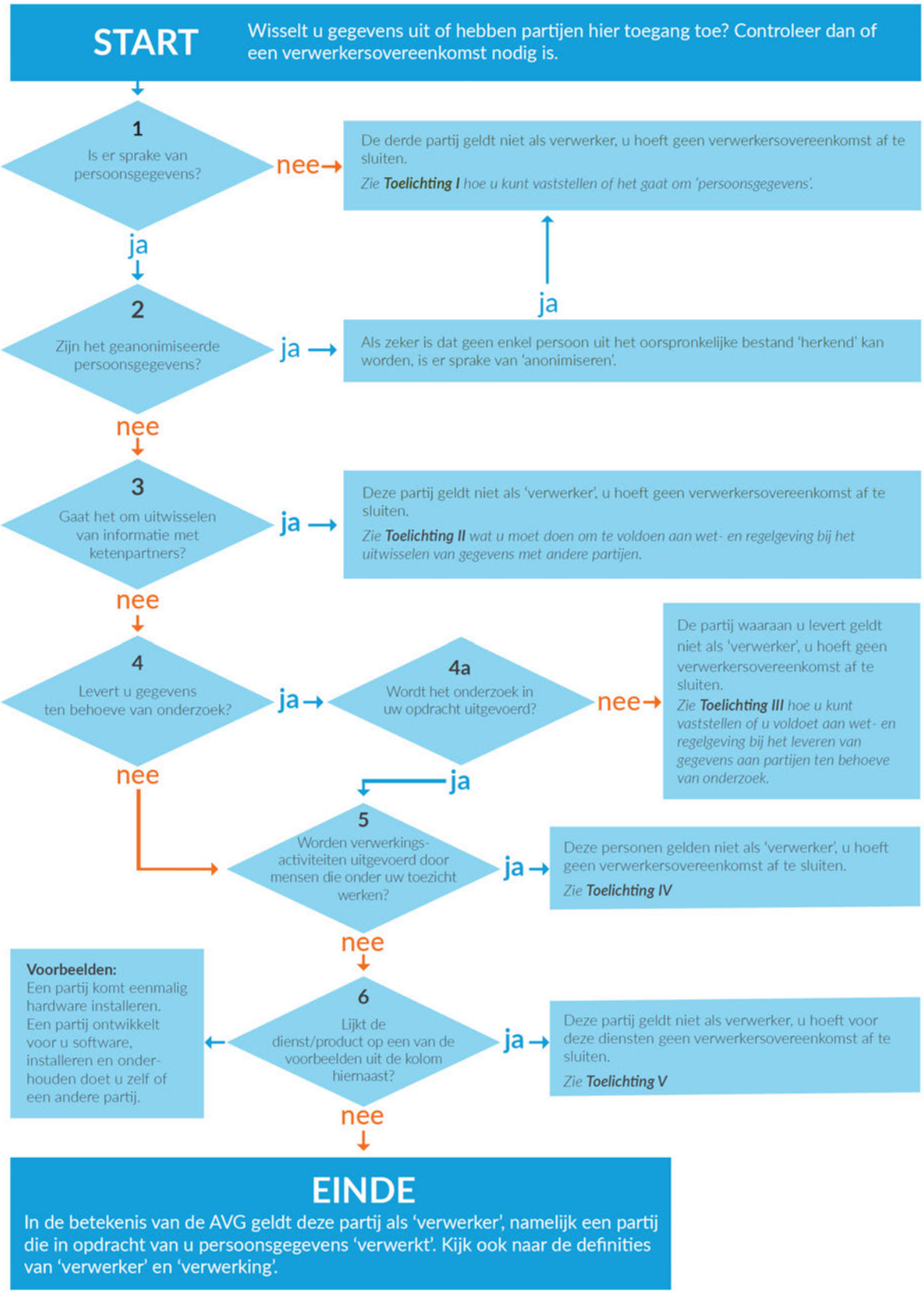
- **Persoonsgegevens**: gegevens die herleidbaar zijn tot individuele personen, zoals gegevens van rechtszoekenden,
  personeelsgegevens en gegevens over aangesloten ketenpartijen en professionele partijen.
- **Verwerking van persoonsgegevens**: elke handeling met betrekking tot persoonsgegevens. Daaronder vallen het verzamelen, bewaren, in de cloud plaatsen, wijzigen, raadplegen, gebruiken, verstrekken, afschermen en vernietigen van persoonsgegevens.
- **Verwerker**: de partij die, in opdracht van een verantwoordelijke, persoonsgegevens verwerkt. Dus eenieder, anders dan de medewerkers of ingehuurd personeel, die toegang heeft tot de persoonsgegevens.
- **Ketenpartij**: andere organisatie die in samenhang met u gegevens verwerkt en waarbij sprake is van een zekere mate van continuïteit van activiteiten. Ketenpartijen hebben hun eigen verantwoordelijkheid voor de door hen verwerkte gegevens.
- **Gegevensuitwisseling:** het uitwisselen van (persoons)gegevens met ketenpartners of medewerkers in relatie tot de procesvoering van een rechtszaak, voor de eigen bedrijfsvoering of voor andere doeleinden zoals onderzoek.
- **Verantwoordelijke**: een natuurlijk- of rechtspersoon die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Bijvoorbeeld het gerecht of de dienst die opdracht heeft gegevens aan een verwerker om persoonsgegevens te verwerken.

Uit de beslisboom blijkt bijvoorbeeld dat voor de volgende partijen een verwerkersovereenkomst nodig is:

- De leverancier en/of beheerder van het informatiesysteem waarin dossier zijn opgeslagen. De leverancier heeft dan toegang tot de gegevens en geldt zodoende als verwerker.
- Het administratiekantoor dat de salarisadministratie verzorgt en hiertoe persoonsgegevens van werknemers moet verwerken.
- Dienstverleners die rapportages maken en hiervoor toegang hebben tot de gegevens van rechtszoekenden en/of medewerkers.
- De beheerder van de telefonie-omgeving waarin gesprekken kunnen worden opgenomen.

In ‘Bijlage: voorbeelden’ is een uitgebreidere lijst van veel voorkomende situaties te vinden waarbij een verwerkersovereenkomst noodzakelijk is.

BESLISBOOM VERWERKERSOVEREENKOMST



TOELICHTING I: PERSOONSGEGEVENS

Persoonsgegevens zijn alle gegevens die direct of indirect herleidbaar zijn tot een individu. Individuen kunnen direct geidentificeerd worden aan de hand van voornaam, achternaam, adres, BSN, etc. Stel dat deze verwijderd worden uit een document maar overige gegevens zoals de inhoud van een hobby, de geboortedatum en woonplaats van betrokkenen zijn nog wel zichtbaar. Voor iemand die de betrokkene kent, zal het niet moeilijk zijn om uit deze gegevens indirect de betrokkene gedeeltelijk te kunnen identificeren.

TOELICHTING II: KETENPARTNERS

Ketenpartijen, zoals het Openbaar Ministerie, de Raad voor de kinderbescherming en het CJIB, zijn geen verwerkers. Deze partijen zijn net als de gerechten verantwoordelijken. Dit betekent dat u geen verwerkersovereenkomst hoeft af te sluiten met deze partijen.

TOELICHTING III: ONDERZOEK EN ANALYSES

U geeft opdracht aan een partij om een analyse uit te voeren op uw bestanden met persoonsgegevens of om een onderzoek uit te voeren. In dat geval geldt deze partij als verwerker en moet u met deze partij een verwerkersovereenkomst afsluiten. Het onderscheidend criterium is dat deze partij op uw verzoek persoonsgegevens verwerkt en niet zelf het doel bepaalt.
Als deze partij echter onder eigen verantwoordelijkheid onderzoek uitvoert (bijvoorbeeld een publieke instantie zoals het WODC, CBS of een universiteit), dan geldt deze partij niet als verwerker maar als verwerkingsverantwoordelijke. U hoeft in dit geval geen verwerkersovereenkomst af te sluiten.

TOELICHTING IV: MEDEWERKERS

Uw medewerkers, al dan niet in vaste dienst, vallen onder uw verantwoordelijkheid en zijn geen verwerkers. Ook ZZP'ers en tijdelijke krachten die op detacheringsbasis bij u werken zijn geen verwerkers.

TOELICHTING V: DIENSTVERLENERS

De termen 'verwerker' en 'verwerken' wekken de suggestie dat een verwerker actief iets doet met de persoonsgegevens. Echter, een bedrijf dat de servers verhuurt waarop u de bestanden met persoonsgegevens bewaart, geldt ook als verwerker. Met deze partij moet u een verwerkersovereenkomst sluiten. Deze partij speelt in uw opdracht een rol bij het verzamelen, vastleggen en wissen van de persoonsgegevens.
Als een partij echt geen toegang kan hebben tot de persoonsgegevens en geen van de activiteiten uitvoert die zijn genoemd in de definitie van verwerken hieronder, is een verwerkersovereenkomst niet nodig. Praktische voorbeelden zijn:

- Een partij die eenmalig op uw locatie hardware komt installeren.
- Een partij die in uw opdracht software ontwikkelt, maar een andere partij die de ontwikkelde software installeert. In dat geval geldt alleen de laatst genoemde partij als verwerker.

BIJLAGE: VOORBEELDEN

In onderstaande tabel staan veel voorkomende voorbeelden van partijen waarmee afspraken worden gemaakt. Mogelijk gelden deze partijen als verwerker en is er een verwerkersovereenkomst nodig. Omdat individuele gevallen kunnen afwijken, is de reden toegelicht waarom er wel of geen verwerkersovereenkomst nodig is. In de eerste kolom staat degene die verantwoordelijk is voor de persoonsgegevens, oftewel vanuit welk perspectief de vraag is benaderd.

Afspraken met (ontvangers)	Verwerkers overeenkomst nodig?	Reden
Software of hardware leverancier	Nee	Wanneer een leverancier alleen de software of hardware levert, maar geen verwerking (bv. toegang) van persoonsgegevens uitvoert, dan is een verwerkersovereenkomst niet nodig. Zie ook: **Toelichting V: dienstverleners**
Zelf management platform leverancier	Ja	Een zelfmanagement platform slaat persoonsgegevens op, bijvoorbeeld inloggegevens. Wanneer u dit platform aan bv. personeel biedt, dan verwerken zij persoonsgegevens onder uw verantwoordelijkheid en is een verwerkersovereenkomst nodig. Zie ook: **Toelichting V: dienstverleners** Indien het platform geen toegang heeft tot persoonsgegevens en onder de verantwoordelijkheid van een ketenpartner wordt aangeboden, dan is een verwerkersovereenkomst niet nodig. De ketenpartij zal dan de verwerkersovereenkomst afsluiten. Zie ook: **Toelichting II: ketenpartij**
Universiteit	Nee	Een universiteit doet zelfstandig onderzoek, niet in opdracht van u. Om persoonsgegevens te delen heeft u wel toestemming nodig. Zie ook: **Toelichting III: onderzoek**
Salaris administratie kantoor	Ja	Wanneer u uw salarisadministratie heeft uitbesteed dan is een verwerkersovereenkomst met deze partij nodig. Zie ook: **Toelichting V: dienstverleners**
Salaris administratie software leverancier	Nee	Wanneer u uw salarisadministratie in eigen beheer voert (eventueel met een ingehuurde salarisadministrateur) en de software- leverancier geen toegang tot gegevens kan krijgen (de software is lokaal geïnstalleerd), dan is een verwerkersovereenkomst niet nodig. Betreft het een 'webapplicatie', dan is een verwerkersovereenkomst wel nodig. De softwareleverancier verwerkt dan persoonsgegevens. Zie ook: **Toelichting V: dienstverleners**
Website beheerder, intranet beheerder of hosting partij	Ja	Wanneer persoonsgegevens worden verwerkt, dan is een verwerkersregister noodzakelijk. Dit is bijvoorbeeld het geval wanneer gebruik wordt gemaakt van een online invulformulier, een mogelijkheid tot aanmelding van een afspraak of een andere invoermogelijkheid waar persoonsgegevens kunnen worden ingevoerd. Zie ook: **Toelichting V: dienstverleners**

Bijlage B: Veel gestelde vragen

Wie zijn binnen de Rechtspraak verantwoordelijk voor het afsluiten van verwerkersovereenkomsten?
Het Landelijk Dienstencentrum Rechtspraak en IVO zijn verantwoordelijk voor het afsluiten van verwerkersovereenkomsten voor Raamcontracten en IT contracten voor landelijke IT applicaties. Gerechten zijn zelf verantwoordelijk voor het afsluiten van verwerkersovereenkomsten met externe leveranciers die zij zelfstandig hebben ingehuurd. Voor vragen kunt u terecht bij privacy@rechtspraak.nl

Moet ik een verwerkersovereenkomst afsluiten met ketenpartijen?
Als u gegevens uitwisselt met ketenpartijen dan is er reeds een wettelijke grondslag voor de uitwisseling van gegevens. Ketenpartijen zijn in die zin zelfstandig verwerkingsverantwoordelijk. Wel dienen er afspraken gemaakt te worden tussen ketenpartijen over de uitwisseling van gegevens. Deze afspraken dienen te worden vastgelegd in zogenoemde convenanten of informatieprotocollen.

Wanneer moet ik een verwerkersprotocol afsluiten met een overheidsdienstverleners?
In sommige gevallen is de Rechtspraak opdrachtgever voor overheidsdienstverleners. Denk hierbij aan BZK voor P-direkt en DFEZ JenV voor Leonardo. In die gevallen is het noodzakelijk dat een zogenoemd verwerkersprotocol wordt vastgesteld.

Moeten wij met een advocaat ook een verwerkersovereenkomst afsluiten?
Met advocaten hoeft geen verwerkersovereenkomst te worden afgesloten. Immers er is hier geen sprake van een relatie opdrachtgever-opdrachtnemer tussen de Rechtspraak en de advocaat of omgekeerd. De Rechtspraak is zelfstandig verwerkingsverantwoordelijk voor de persoonsgegevens en de advocaat ook.
Ook als de advocaat diensten afneemt van de Rechtspraak, zoals portaaldiensten, hoeft de advocaat geen verwerkersovereenkomst af te sluiten met de Rechtspraak. Wel dienen er afspraken te worden vastgelegd over het gebruik van bepaalde voorzieningen en diensten (zoals de portal) door de advocaat.

Moeten met deskundigen en tolken verwerkersovereenkomsten worden afgesloten?
Nee, met deskundigen en tolken hoeft geen verwerkersovereenkomst te worden afgesloten. Zij zijn zelfstandig verantwoordelijk voor de verwerking van persoonsgegevens van cliënten. Wel is het uiteraard van belang met deskundigen en tolken afspraken te maken over geheimhouding en bewaartermijnen.

Moeten mediators en coaches verwerkersovereenkomsten afsluiten?
Mediators en coaches hoeven eveneens geen verwerkersovereenkomst af te sluiten met de Rechtspraak. Alhoewel mediators en coaches in opdracht handelen van de Raad voor de rechtspraak, heeft de opdracht geen betrekking op de wijze van verwerken van persoonsgegevens. Mediators en coaches zijn zelfstandig verantwoordelijk voor de verwerking van persoonsgegevens van cliënten. Als de rechtspraak mediation of coaching aanbiedt aan medewerkers of rechtszoekenden, is het uiteraard wel van belang dat de Rechtspraak zich ervan ver gewist dat met de mediators en coaches afspraken worden gemaakt over de vertrouwelijkheid van gegevens.

Moeten voor externe cursussen en opleidingen verwerkersovereenkomsten worden afgesloten?
Hiervoor geldt hetzelfde als voor mediation en coaching. Het opleidingsinstituut is zelfstandig verwerkingsverantwoordelijk voor de vertrouwelijkheid van persoonsgegevens door cliënten.
Het is van belang bij het inschakelen van het externe instituut goede afspraken te maken over de vertrouwelijkheid en bewaartermijnen van gegevens. Hierbij is met name van belang te beseffen dat examengegevens gezien kunnen worden als gevoelige persoonsgegevens die iets zeggen over het functioneren van personen. Daarom is het van belang daar extra goede afspraken over te maken.

Document 7:
20210913 Privacybeleid Rechtspraak

Privacybeleid Rechtspraak

Inleiding
Het hier beschreven Privacybeleid werkt de algemene strategische visie van de Rechtspraak ten aanzien van privacy verder uit. Het doel hierbij is dat de Rechtspraak de privacywet- en privacyregelgeving naleeft.

Doelstelling
Bescherming van de persoonlijke levenssfeer acht de Rechtspraak van groot belang. De Rechtspraak verwerkt persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), de bijbehorende Uitvoeringswet AVG (UAVG), de Wet Justitiële en Strafvorderlijke Gegevens (Wjsg) en overige wet- en regelgeving. Om te zorgen dat in lijn met de hiervoor genoemde wet- en regelgeving word gehandeld, bevat het strategisch plan privacy verschillende conclusies en actiepunten voor het gebruik van persoonsgegevens en de bescherming hiervan.

De actiepunten uit het strategisch privacy plan zijn verder uitgewerkt in het privacy borgingsplan. Indien nieuwe actiepunten worden geconstateerd worden deze aan het borgingsplan toegevoegd. Met dit borgingsplan laat de Rechtspraak zien te werken aan haar doelstelling om in lijn met de privacywet- en privacyregelgeving te acteren.

Definities
De definities van veel voorkomende begrippen staan beschreven in de AVG en de Wjsg.

Toepassingsbereik
Dit Privacybeleid geldt voor alle verwerkingen van persoonsgegevens door medewerkers van de Rechtspraak voor zover die vallen onder de verantwoordelijkheid van hun taken.

Wie is verantwoordelijk?
Verantwoordelijken voor de verwerking van persoonsgegevens zijn volgens de AVG en de Wjsg 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’. De specifieke verantwoordelijkheden zijn nader omschreven in het beleidskader *Privacy Governance Rechtspraak en het bijbehorende addendum*. De Raad voor de rechtspraak en de gerechten kunnen te allen tijde aantonen dat ze de beginselen en rechtsgrondslagen naleven.

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 Wjsg 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 organisaties die onderdeel zijn van de Staat der Nederlanden bijvoorbeeld is het afsluiten van een verwerkersovereenkomst niet nodig. In dat geval wordt een ‘verwerkersprotocol’ opgesteld wanneer sprake is van een verwerkersrelatie.

Beginselen
Diegenen door hun functie verantwoordelijk zijn voor het verwerken van persoonsgegevens doen dat in overeenstemming met de beginselen van de AVG en de Wjsg. De gerechtsbesturen en de Raad zijn verantwoordelijk voor de inrichting van processen en systemen volgens deze beginselen. De beginselen zijn:

- Rechtmatig (op basis van doelen die hun grondslag vinden in wet- en regelgeving);
- Behoorlijk (verwerking van persoonsgegevens is eerlijk en zorgvuldig);
- Transparant (verantwoording- en informatieplicht richting betrokkenen en de samenleving);
- Doelbinding (gegevens worden verzameld voor gerechtvaardigde doeleinden);
- Dataminimalisatie (niet meer persoonsgegevens dan strikt noodzakelijk voor het doel van verwerking);
- Opslagbeperking (niet langer dan noodzakelijk of wettelijk toegestaan voor het doel van verwerking);
- Juistheid (de juistheid van gegevens wordt gecontroleerd en indien nodig vinden correcties plaats);
- Integriteit en vertrouwelijkheid (geborgd door passende beveiligingsmaatregelen);
- Verantwoordingsplicht (het kunnen aantonen van de naleving van bovengenoemde beginselen).

Grondslagen voor rechtmatige verwerking
De verwerking van persoonsgegevens is op basis van de AVG alleen rechtmatig als aan een van de in artikel 6 lid 1 van de AVG genoemde voorwaarden is voldaan. Bij de grondslagen uit artikel 6 AVG moeten twee opmerkingen gemaakt worden:

- Gebruik van de grondslag ‘toestemming’ (sub a) is niet toegestaan wanneer sprake is van een ongelijke verhouding (een wanverhouding). Dit geldt met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, zoals de Rechtspraak. Het is dan onwaarschijnlijk dat de toestemming vrijelijk verleend is.
- De grondslag ‘gerechtvaardigd belang’ (sub f) is niet toegestaan voor de verwerking van persoonsgegevens door overheidsinstanties in het kader van de uitoefening van hun publieke taken.

De Wjsg voegt in artikel 3 Wjsg een grondslag toe voor het verwerken van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Daartoe behoort ook de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Bij de introductie van nieuwe processen of nieuwe systemen toetsen de gerechtsbesturen, de Raad en de landelijke diensten of aan (een van de) grondslagen voor rechtmatige verwerking wordt voldaan. Als het gaat om de bestaande processen en systemen doen zij dat periodiek. Voor de uitoefening van primaire taken is geen toestemming nodig voor het verwerken van persoonsgegevens door betrokkene.

Soorten persoonsgegevens
De Rechtspraak kan bij haar werkzaamheden alle mogelijke categorieën van persoonsgegevens verwerken. Hierbij valt te denken naam, adres, woonplaats, telefoonnummer, geboortedatum, emailadressen, financiële persoonsgegevens, bankrekeningnummers, paspoortkopieën, foto’s, bijzondere persoonsgegevens zoals medische gegevens, strafrechtelijke persoonsgegevens en bij wet voorgeschreven identificatienummers (BSN).

Uitzonderingen AVG

- De AVG is niet van toepassing bij verwerking van gegevens door een bevoegde autoriteit met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Hiervoor is de Richtlijn van toepassing. De Richtlijn is uitgewerkt in de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Wet politiegegevens (Wpg).
- De AVG (artikel 23, lid 1) biedt de mogelijkheid gemotiveerd af te wijken van de rechten van betrokkenen zoals het recht van inzage, correctie of de meldplicht datalekken en/of deze rechten te beperken. Dat kan alleen als een van de uitzonderingsgronden van toepassing is.

- Mocht dat het geval zijn dan moet de Rechtspraak volgens de AVG (artikel 23, lid 2) wel aangeven hoe de rechten en vrijheden van betrokkenen met betrekking tot de persoonsgegevens worden geborgd. Ook moet de Rechtspraak aangeven of en hoe betrokkenen worden geïnformeerd over de beperkingen van rechten en plichten.

Algemene verplichtingen

De Raad voor de rechtspraak, de gerechten en de landelijke diensten hebben een aantal algemene verplichtingen waaraan zij moeten voldoen op basis van de AVG en de WJSG. Die algemene verplichtingen zijn bedoeld te waarborgen en te kunnen aantonen dat de Rechtspraak persoonsgegevens verwerkt in overeenstemming met de AVG en de WJSG.
Deze algemene verplichtingen zijn:

1. Het voeren van een actief privacybeleid;
2. Het verwerken van toereikende gegevens op basis van een doelstelling.
3. Het voeren van een actief beveiligingsbeleid;
4. Het houden van een register van verwerkingen;
5. Het uitvoeren van Privacy Impact Assessments (PIA);
6. Het doorvoeren van privacy door ontwerp en standaardinstellingen (privacy by design);
7. Het nemen van technische en organisatorische beveiligingsmaatregelen ter voorkoming van ongeoorloofde of onrechtmatige verwerking
8. Melding van een inbreuk in verband met persoonsgegevens (datalekken);
9. Het uitvoering geven aan rechten van betrokkenen;
10. Het sluiten van verwerkersovereenkomsten;
11. Het vaststellen van verantwoordelijkheden van gezamenlijk verwerkingsverantwoordelijken;
12. Het aanwijzen van een functionaris gegevensbescherming;
13. Het samenwerken met toezichthoudende autoriteiten;
14. Het opstellen van of aansluiten bij gedragscodes en certificering;

De concrete invulling van deze algemene wettelijke verplichtingen binnen de Rechtspraak zijn in meer in detail omschreven in de *Minimumnormen privacy*.

Specifieke maatregelen

Naast algemene verplichtingen zijn er ook specifieke onderwerpen en processen waar privacy maatregelen gelden ter bescherming van persoonsgegevens:

1. De verzameling en registratie van gegevens (invoer, correctie, verwijdering, combineren, etc.);
2. Het bewaren en archiveren van gegevens;
3. Het autoriseren van medewerkers;
4. De uitwisseling van gegevens met procespartijen, ketenpartijen, professionele partijen en derden;
5. Het verwerken van gegevens ten behoeve van wetenschappelijk, statistisch en historisch onderzoek;
6. Doorgiften van persoonsgegevens aan derde landen of organisaties;
7. Het verstrekken van gegevens aan de pers;
8. De publicatie van registers en uitspraken;
9. De openbaarheid van bestuur;
10. Nieuwsbrieven;
11. Het gebruik websites en cookie;
12. Big data en open data;
13. Postverwerking;
14. Vernietiging gegevensdragers (papier en digitaal).

Gerechten en diensten zorgen ervoor dat bovengenoemde onderwerpen en processen voldoen aan de AVG en de Richtlijn en de daaraan verwante wet- en regelgeving. De normen die voor de privacy maatregelen hierbij van toepassing zijn staan beschreven in de *Minimumnormen privacy*.

Middelen
Gekoppeld aan het privacybeleid voorzien de Raad voor de rechtspraak en de gerechtsbesturen voldoende en aantoonbaar in de benodigde middelen om te kunnen voldoen aan het privacybeleid; waaronder:

- De middelen voor interne bewustwording en doelgroepgerichte training van medewerkers op privacybestendig werken;
- De middelen voor het faciliteren van transparantie voor betrokkenen (zoals inzage);
- De (technische) mogelijkheid om persoonsgegevens te kunnen corrigeren;
- De (technische) mogelijkheid om persoonsgegevens te anonimiseren of verwijderen;
- De middelen voor adequate beveiliging van persoonsgegevens
- De middelen voor adequaat en onafhankelijk toezicht.

Interne bewustwording, kennisdeling en educatie
Om er voor te zorgen dat de AVG en de Richtlijn worden nageleefd is het stimuleren van interne bewustwording, kennisdeling en educatie van belang. Op de privacypagina op landelijk Intro delen we informatie, beleid en kennis. Dat doen we ook via MKO en Wiki-pagina's.

Tot slot bieden de gerechten en diensten hun medewerkers de mogelijkheid in- en externe cursussen en opleidingen te volgen. Daarin wordt samen gewerkt met onder meer de SSR en het LDCR, ook voor wat betreft de educatie van raadsheren, rechters en juridische ondersteuning.

Gedragscode
Een organisatie kan ervoor kiezen om een gedragscode op te stellen. In een gedragscode worden de eisen van de AVG voor een specifieke branche uitgewerkt tot concreet te nemen maatregelen om aan de AVG te voldoen. Door de Rechtspraak wordt niet aangesloten bij een gedragscode.

Interne afstemming en besluitvorming
Privacybeleid heeft continue zorg en aandacht nodig. Om er voor te zorgen dat de Rechtspraak dit beleid invoert, borgt, uniform toepast en structureel verbetert is er regelmatig overleg met de privacyfunctionarissen van gerechten en diensten en de landelijk functionaris gegevensbescherming.

Zo nodig richt de Rechtspraak werkgroepen op om bepaalde zorgen en aandachtspunten te bespreken of om bepaalde delen van het beleid verder uit te werken. Afhankelijk van het onderwerp wordt bekeken in hoeverre de privacy coördinatoren zelf binnen de gerechten aanpassingen kunnen doorvoeren of dat besluitvorming door de Raad en/of presidenten van gerechten nodig is. Er wordt dan gebruik gemaakt van de bestaande overlegstructuren en procedures voor besluitvorming.

Externe verantwoording- en informatie
Om betrokkenen, professionele partijen en andere extern geïnteresseerden te informeren over de wijze waarop de Rechtspraak invulling geeft aan de AVG en de WJSG staat op Rechtspraak.nl een webpagina 'Privacy'. Hier staat onder meer de privacyverklaring, is te lezen welke persoonsgegevens de Rechtspraak verwerkt en welke rechten betrokkenen hebben met betrekking tot hun persoonsgegevens. Het bureau Raad is verantwoordelijk voor het beheer van dit onderdeel op Rechtspraak.nl in samenwerking met het team content van het LDCR en functionarissen bij IVO.

Uitwisseling van gegevens met externe partijen

De Rechtspraak wisselt persoonsgegevens uit met procespartijen, ketenpartijen, professionele partijen en derden, bijvoorbeeld het OM, het CJIB, DJI en de Raad voor de Kinderbescherming. De uitwisseling van gegevens met deze externe partijen moet voldoen aan de AVG en de WJSG. De verzendende partij is in beginsel verantwoordelijk voor hetgeen hij indient bij de Rechtspraak. Het enkele feit dat een gerecht de documenten conform procesrecht doorstuurt doet hier niets aan af, behoudens de volgende uitzonderingen:

1. Persoonsgegevens die voor eigen (administratieve) doeleinden door de Rechtspraak zijn opgevraagd en zijn ontvangen van de verzendende partij en/of zijn verrijkt en vervolgens zijn doorgestuurd terwijl dit niet de bedoeling was. De verantwoordelijkheid strekt zich dan uit tot de behandeling van de ontvangen en verrijkte informatie. Persoonsgegevens die zijn ontvangen van een procespartij en door de Rechtspraak naar verkeerde personen zijn verstuurd. De verantwoordelijkheid strekt zich dan uit tot het herstel en afhandeling van de verkeerd verstuurde informatie.
2. Persoonsgegevens die zijn ontvangen van een procespartij en door de Rechtspraak naar de juiste partij zijn doorgestuurd, maar de verzendende partij heeft tijdig aangegeven dat de stukken teveel of onjuiste persoonsgegevens bevatten. Op schriftelijk verzoek van partijen wordt het stuk vernietigd. Het is dan de verantwoordelijkheid van de betreffende partij om tijdig een gecorrigeerde versie te doen toekomen.
3. De Rechtspraak heeft daarnaast een contextafhankelijke zorgplicht om (keten-)partijen te wijzen op eventuele privacy-inbreuken wanneer die worden gesignaleerd. Dit betekent echter niet dat de gerechten actief documenten dienen te controleren.

De Rechtspraak heeft daarnaast een contextafhankelijke zorgplicht om (keten-)partijen te wijzen op eventuele privacy-inbreuken wanneer die worden gesignaleerd. Dit betekent echter niet dat de gerechten actief documenten dienen te controleren.

Indien nodig worden er afspraken gemaakt om de bescherming van persoonsgegevens in de keten te garanderen. Daarvoor wordt eveneens aangesloten bij overheidsbrede standaarden, zoals de Baseline Informatiebeveiliging Overheid (BIO). Over de uitvoering van deze afspraken worden de gerechten op de hoogte gehouden. Ook wordt hen nadrukkelijk gevraagd om mee te werken aan de uitvoering van de afspraken.

Controle en toezicht

Om de privacywet- en privacyregelgeving blijvend te borgen in de organisatie is inrichting van een managementproces nodig. De verwerkingsverantwoordelijke heeft de wettelijke plicht passende technische en organisatorische maatregelen te nemen om te waarborgen en te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de wet- en regelgeving is. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd. Om aan deze verplichting te voldoen richten de gerechten en diensten een PDCA-cyclus (plan-do-check-act) in.

Het basisdocument in deze PDCA-cyclus is een actieplan met daarin algemene activiteiten, bevindingen en acties. Te denken valt aan:

- Planfase (plan): inventariseren bevindingen en voorstellen acties en maatregelen (privacy by design);
- Uitvoeringsfase (do): implementeren en uitvoeren van maatregelen;
- Controle (check): controleren op het bestaan en werking van maatregelen;
- Verbeterfase (act): het voorstellen van verbeteringen op de korte en langere termijn.

Binnen de gerechten is dit een taak van de privacy coördinatoren. Op landelijk niveau verzorgt het bureau BVA de landelijke PDCA-cyclus die tweejaarlijks plaatsvindt. Toezicht op deze procedures is onderdeel van de taken van de landelijk functionaris gegevensbescherming.

Administratieve organisatie en interne controle

Uit de AVG vloeit voort dat de Rechtspraak kan aantonen de AVG na te leven.
Dat kan door de aanleg van een register van verwerkingen, een register van datalekken, een register voor verzoeken betrokkenen, privacy impact assessments en (verwijzingen naar) beleid en ontwerpdocumentatie. Op basis van deze administratieve organisatie vindt interne controle plaats. De gerechtsbesturen en de Raad zijn verantwoordelijk voor deze interne controle. Zie hiervoor PN – 08 - Minimumnorm privacy – Intern toezicht.

Planning en verantwoording
De gerechten en diensten worden aangeraden jaarlijks de plannen met betrekking tot privacy management op te nemen in het jaarplan en de jaarrapportage. Op dit moment is dat nog geen verplichting.

Accountantscontrole en auditing
De opzet van de accountantscontrole of eventuele audits naar de naleving van de AVG en de WJSG beschrijven we hier niet verder. We volstaan met het verwijzen naar afspraken met de accountant over de inrichting van de accountantscontrole en het auditbeleid.

Extern toezicht en rechtsbescherming
In hoofdstuk VI tot en met VII van de AVG en in de WJSG wordt de inrichting van het externe toezicht en de rechtsbescherming neergelegd. Voor de Rechtspraak geldt vanwege haar onafhankelijk positie in het staatsbestel een bijzondere situatie. Voor de gerechten geldt de *"Regeling toezicht verwerking persoonsgegevens AVG Hoge Raad"* en voor de bestuursrechtelijke colleges geldt de *"Regeling toezicht verwerking persoonsgegevens AVG Bestuursrechtelijke colleges"*.

Vaststelling privacybeleid
Dit beleidskader is oorspronkelijk vastgesteld door de Raad voor de rechtspraak en de Presidentenvergadering op mandaat van de gerechtsbesturen op 25 mei 2018. Het is vervolgens geactualiseerd in het kader van de actualiseringscyclus van het handboek Integrale Veiligheid (2019), het opstellen van de Minimumnormen Privacy (2020) en de beschrijving van de verantwoordelijkheden inzake het uitwisselen van documenten met procespartijen (2021).

Document 8:
Interne Procedure Rechten Betrokkene

Interne Procedure Rechten Betrokkene

(versiedatum: 25 mei 2018)

Introductie

De Algemene Verordening Gegevensbescherming kent aan de betrokkene een aantal rechten toe, op grond waarvan zij een verzoek kunnen indienen dat betrekking heeft op hun persoonsgegevens. Om vanaf 25 mei a.s. gehoor te kunnen geven aan dergelijke verzoeken is het van belang dat er een landelijke procedure is die houvast biedt aan de gerechten en andere organisatieonderdelen. Transparantie, klantvriendelijkheid en behoorlijke bejegening staan binnen de procedure betrokkenen centraal. Ten aanzien van externe communicatie over de procedure rechten betrokkene staat op Rechtspraak.nl een privacyverklaring en uitleg over op welke wijze betrokkenen hun rechten ontleend aan de AVG kunnen uitoefenen. Tevens is een formulier op de website gepubliceerd, dat de betrokkene kan gebruiken om een verzoek in te dienen. Een overzicht van mogelijke verzoeken is in *Tabel A* opgenomen.

Dit stuk bespreekt stapsgewijs de interne procedure en gaat nader in op de wijze waarop de gerechten om kunnen gaan met verzoeken van betrokkenen. De projectgroep hoopt met deze handreiking een basis te bieden aan alle gerechten. Uiteraard zullen ervaringen en de werkelijke gang van zaken in de praktijk dit document nuanceren. Wij geven u mee dat deze handreiking primair is geschreven vanuit het perspectief van bedrijfsvoering en niet zozeer ten aanzien van het 'rechterswerk'/primaire proces (behandeling ter zitting). Er is sprake van samenloop wanneer het informatieverzoek onder de AVG raakt aan de thans bestaande inzageprocedures en/of betrokkene doelt op een ander dan een verzoek op grond van de AVG, maar de verkeerde duiding heeft gegeven[1]. In dat geval moet goed bekeken worden welke procedure de betrokkene voor ogen heeft en of het niet meer voor de hand ligt de reeds bestaande inzage- of klachtenprocedure te volgen.

De interne procedure is onderverdeeld in zeven fases:

Fase 1: Ontvangen van verzoek
Fase 2: Identificeren van betrokkene
Fase 3: Reageren op verzoek (ontvangstbevestiging)
Fase 4: Behandelen van verzoek
Fase 5: Beantwoorden (inhoudelijk)
Fase 6: Archiveren van verzoeken
Fase 7: Klachten

[1] Art. 843a Rv, art 12/30-34 Sv, art. 7:18 Awb, Wob-verzoek, klacht.

Fase 1: Ontvangst verzoek

Een verzoek kan op diverse wijzen binnen komen. Bij voorkeur vult de betrokkene het privacyformulier op de website in. Hoewel het formulier de meest wenselijke weg is, is het niet uitgesloten dat verzoeken ook op andere wijzen worden ingediend, bijvoorbeeld middels een 'gewone brief', of via de behandelend rechter. In die gevallen kan de betrokkene gewezen worden op het verzoekformulier op de website. Denkbaar is dat het verzoek voldoende informatie bevat om het in behandeling te nemen. Dan is verwijzing naar het formulier niet nodig, maar kan wel gevraagd worden om nadere informatie (een preciseringsverzoek. Daarover later meer in fase 3).

Op de website van rechtspraak.nl staat vanaf 25 mei de volgende tekst over indienen van verzoeken:

Formulier privacyverzoeken
U kunt het formulier privacyverzoeken per post sturen naar het gerecht waar uw rechtszaak diende of naar de Raad voor de rechtspraak t.a.v. de coördinator informatieverzoeken[2]. Wij mogen u op basis van dit formulier alleen maar informatie verstrekken over uw eigen persoonsgegevens en niet over andere betrokkenen. >Adressen Rechtspraak.

Het formulier is niet bedoeld voor reguliere inzage in het dossier van een lopende rechtszaak
Het formulier privacyverzoeken is niet bedoeld voor "reguliere inzage" in het dossier van een lopende rechtszaak. In dat geval kunt u of uw advocaat zich rechtstreeks wenden tot het gerecht waar uw zaak loopt met het verzoek om een "reguliere inzage".

Rechtspraak Service Centrum
Als u vragen heeft over het formulier of de afhandeling van uw verzoek, kunt ook bellen met het Rechtspraak Service Centrum. Het RSC is bereikbaar van 08.00 tot 20.00 op telefoonnummer 088 3616161.

Identificatieplicht
De Rechtspraak registreert vaak gevoelige gegevens. Als u verzoekt om een overzicht van persoonsgegevens of als u gegevens wilt wijzigen, dan is het nodig dat wij zeker weten wie u bent, voordat wij aan uw verzoek kunnen voldoen. Dit om te voorkomen dat wij uw gegevens zomaar wijzigen of aan iemand anders geven. Daarom zal een medewerker van de Rechtspraak (per brief of telefoon) contact met u opnemen en u vragen om u aan de balie van een gerecht in uw woongebied te komen legitimeren met een geldig identificatiebewijs. Na uw identificatie wordt uw verzoek direct (of zo snel mogelijk) verwerkt.

Kosten
De Rechtspraak brengt in beginsel geen kosten in rekening voor de afhandeling van uw verzoek. Als uw verzoek echter zeer omvangrijk is, kan aan u gevraagd worden om een redelijke vergoeding.
Deze zal worden bepaald afhankelijk van de omvang van het verzoek.

Wilt u een klacht indienen?
Heeft u een klacht over de verwerking van uw persoonsgegevens, dan kunt een klacht indienen bij de toezichthoudende autoriteit. Voor klachten over de verwerking van uw persoonsgegevens in rechtszaken kunt u een klacht indienen bij de Procureur Generaal bij de Hoge Raad. Klik hier [link] voor contactgegevens. Voor klachten over alle overige verwerkingen van persoonsgegevens kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Klik hier [link] voor de contactgegevens.

Voor de bestuursrechtelijke colleges (Afdeling bestuursrechtspraak Raad van State, Centrale Raad van Beroep en het College van Beroep voor het bedrijfsleven) geldt een aparte regeling welke beschreven staat op de websites van de betreffende colleges.

[2] Onderzocht wordt hoe op termijn schriftelijke verzoeken ook via het RSC kunnen worden ingediend.

Verzoeken die ontvangen worden, moeten onverwijld worden doorgestuurd naar de **lokale coördinator informatieverzoeken (LCI) van het betreffende gerecht of landelijke dienst**[3].

Om deze reden is het van groot belang dat medewerkers binnen het gerecht het verzoek kunnen herkennen en dat iedereen op de hoogte is wie de behandelend functionaris is binnen het gerecht. Bij het verkennen van een verzoek - als zijnde een verzoek in het kader van de AVG of Richtlijn - kan het helpen aan te geven op welke woorden medewerkers moeten letten, bijvoorbeeld: AVG, Richtlijn, persoonsgegevens, privacy, etc. (woordweb). Het is de bedoeling dat u aan de baliemedewerkers een formulier ter beschikking stelt dat door betrokkenen kan worden ingevuld als zij zich komen identificeren aan de balie. Daarbij krijgen de baliemedewerkers ook het formulier privacyverzoeken mochten betrokkenen spontaan een verzoek willen doen en daarom vragen aan de balie.

Overigens is het bestuur van het gerecht formeel bevoegd en verantwoordelijk voor de afhandeling van het verzoek. Na doorverwijzing door het RSC of medewerkers van gerechten of diensten, spelen de lokale en landelijke coördinatoren een belangrijke rol om ervoor zorg te dragen dat het verzoek **klantvriendelijk, begrijpelijk en zo volledig mogelijk** wordt afgehandeld. **De bejegening** van de betrokkene staat daarbij centraal. Als een verzoek wordt afgewezen dan is het van belang dat te doen op een wijze die begrijpelijk is voor de betrokkene. Ook dit is een vereiste van de AVG en Richtlijn.

De **centraal coördinator informatieverzoeken (CCI)** dient van ieder verzoek, ongeacht waar het binnen komt, op de hoogte gebracht te worden. Dat kan naar het mailadres privacy@rechtspraak.nl. Het is niet de bedoeling om het gehele verzoek door te sturen, tenzij het een algemeen verzoek is dat de betrokkene bijvoorbeeld wil weten “welke gegevens de Rechtspraak van hem verwerkt” en niet nader wil preciseren waar hij/zij naar op zoek is. Een algemene beschrijving met duiding van het verzoek zonder vermelding van persoonsgegevens volstaat.
Het is van belang het door te sturen naar de CCI om te zorgen dat verzoeken uniform worden afgehandeld, om van elkaar te kunnen leren en te monitoren welke verzoeken er binnen komen.

Op de Intropagina privacy is een contactenlijst gepubliceerd waarop per gerecht de namen van coördinatoren zijn vermeld om doorverwijzingen te bespoedigen en onderlinge afstemming mogelijk te maken.

a. *Samenwerking LCI’s en CCI’s:* Indien de LCI constateert dat het verzoek betrekking heeft op een ander gerecht, stuurt de LCI het verzoek door naar de LCI van dat andere gerecht en informeert altijd de Centraal Coördinator Informatieverzoeken over de doorzending. De CCI coördineert gerecht overstijgende verzoeken en adviseert de gerechten in complexe kwesties. In het kader van coördinatie/monitoring en advies dient de LCI de CCI te informeren ten aanzien van alle verzoeken die bij zijn/haar gerecht zijn ingediend. Daarnaast is in deze beginfase het aspect dat gerechten van elkaar kunnen leren (kennisdeling) van belang. Bekeken moet worden hoe dat in de praktijk tot uiting komt. In ieder geval kunnen zaakgegevens worden geanonimiseerd. De CCI kan op zijn/haar beurt een beroep doen op de Functionaris Gegevensbescherming (hierna: FG). Een schematisch overzicht (*Beslisboom*) is te vinden in de bijlage.

[3] Aan wie de taak van lokale coördinator informatieverzoeken binnen het gerecht wordt gedelegeerd, staat ter vrije bepaling van de gerechten. Onze suggestie is om de functie onder te brengen bij een reeds bestaande functie, zoals de Klachtenfunctionaris, Bestuurssecretaris of de Privacy Coördinator.

b. Indien het verzoek is gericht aan meerdere gerechten, stuurt de LCI het verzoek door naar de CCI, die de doorsturing verzorgt.
c. Voor zover het verzoek betrekking heeft op het eigen gerecht, dan vervolgt de LCI het stappenplan.

Fase 2: Identificatie betrokkene

Nadrukkelijk is het niet zo dat de betrokkene zich eerst moet identificeren voordat het verzoek in behandeling wordt genomen. We nemen het verzoek in behandeling en gaan dan als een speer ervoor zorgen dat we antwoord krijgen op de vraag. Zodoende wordt voorkomen dat het verzoek door louter tijdsnood niet binnen de vereiste termijn (in beginsel 1 maand) kan worden beantwoord. Pas als de betrokkene echter zich is komen identificeren (bij voorkeur ter plekke bij het gerecht) kunnen we het verzoek definitief afdoen. **Het verzoek wordt dus direct na ontvangst van het verzoek in behandeling genomen, maar pas ingewilligd/informatie wordt pas verstrekt op het moment dat de identiteit van betrokkene met zekerheid is vastgesteld.**

Betrokkene kan slechts een verzoek indienen voor zover het betrekking heeft op zijn/haar eigen gegevens, zodat de identiteit op deugdelijke wijze dient te worden vastgesteld. Het vragen van een kopie paspoort is (1) een onrechtmatige verwerking, want de grondslag ontbreekt, (2) een kopie is geen wettig document aan de hand waarvan betrokkene zich kan identificeren, omdat vervalsingen moeilijk zichtbaar kunnen zijn en simpelweg niet controleerbaar is of de betrokkene daadwerkelijk ook de verzoeker c.q. de persoon die het verzoek heeft gestuurd is. Idealiter identificeert betrokkene zich via DigiD, maar zover is het nog niet. Wegens de gevoelige aard van de persoonsgegevens van betrokkene die de Rechtspraak mogelijk verwerkt, is fysieke identificatie aan de balie van het gerecht momenteel de enige mogelijkheid. Dit geldt in de gevallen waarbij betrokkene het verzoek fysiek overhandigt aan de balie (dan kan direct om identificatie worden gevraagd), alsook voor per post of digitaal ingediende verzoeken. In dat geval kan de LCI wijzen op de eis van identificatie aan de balie. Voor betrokkene dient het mogelijk te zijn zich te identificeren bij het dichtstbijzijnde gerecht.

De baliemedewerker noteert de naam van betrokkene, de datum van identificatie en aan welk gerecht het verzoek is gericht. Daartoe is een formulier identificatie opgesteld. In het kader van termijnbewaking, rapportering/monitoring en dossieropbouw is de datum van indiening belangrijk (Zie fase 6).[4] Deze informatie, tezamen met evt. een fysiek verzoek, komen bij de LCI terecht, die het verzoek ofwel (1) in behandeling neemt, (2) of uitzet naar het gerecht waaraan het verzoek is gericht (+ inlichten CCI over doorzending) of (3) doorstuurt naar de CCI omdat het verzoek op meerdere gerechten betrekking heeft.

Wettige Identificatiebewijzen

De reikwijdte van de AVG beperkt zich niet tot de landsgrenzen van Nederland. De bescherming die door deze verordening wordt geboden, heeft betrekking op natuurlijke personen, ongeacht hun nationaliteit of verblijfplaats, in verband met de verwerking van hun persoonsgegevens. Ingeval de betrokkene een ander dan een Nederlandse ingezetene betreft, volstaat identificatie met Europese of internationaal goedgekeurde en geldige[5] identiteitsbewijzen. Ten aanzien van een betrokkene die Nederlandse ingezetene is, volstaan de volgende identificatiebewijzen:

- Een geldig Nederlands rijbewijs;
- Een gemeentelijke identiteitskaart (VNG-model) of Europese identiteitskaart;

[4] Het kan immers voorkomen dat een verzoek van betrokkene onverhoopt aanleiding uitmondt in een klacht van betrokkene.
[5] Via deze link zijn handige tips te vinden voor de beoordeling of een document echt en geldig is.

- Een geldig reisdocument, als bedoeld in art.2 lid 1 van de Paspoortwet (Stb. 1991, 498) (bijv. een geldig nationaal, diplomatiek of dienstpaspoort, of een reisdocument voor vluchtelingen/ vreemdelingen);
- Een document waarover een vreemdeling ingevolge de Vreemdelingenwet 2000 (Stb 2000, 495) moet beschikken.

De projectgroep realiseert zich dat niet gangbare / afwijkende identificatiedocumenten de nodige vragen kan oproepen. Het gaat erom dat identificatie zorgvuldig geschiedt. Bij twijfel kan altijd contact worden gezocht met bijvoorbeeld de Vreemdelingenkamer van het gerecht, de lokale BVC-er of de CCI.

Minderjarigen en andere bijzondere betrokkenen

Denkbaar is dat een verzoek wordt ingediend door een vertegenwoordiger van betrokkene, bijvoorbeeld voogd/ouder van een minderjarige, curator van een onder curatele geplaatste, mentor, bewindvoerder, advocaat namens cliënt etc. Om te borgen dat het verzoek daadwerkelijk voor de betrokkene is ingediend, moet de vertegenwoordiger aantonen dat hij/zij bevoegd is betrokkene te vertegenwoordigen. (art. 3:60 BW – volmacht). Voorts is denkbaar dat bestuurders of personen die een personenvennootschap drijven (eenmanszaak, vof) een informatieverzoek indienen in de hoedanigheid van 'ondernemer van het bedrijf'. Hoewel zij indirect tot natuurlijke personen herleidbaar zijn, kan de Rechtspraak alleen informatieverzoeken t.a.v. natuurlijke personen in behandeling nemen.

Een ouder kan de rechten uit de AVG van zijn/haar kind uitoefenen indien die ouder de wettelijk vertegenwoordiger is. Dat is wanneer die ouder het gezag over het kind heeft. Bij twijfel of de ouder het gezag heeft kan de ouder gevraagd worden om een recent afschrift van de geboorteakte, in combinatie met een recent uittreksel uit het gezagsregister.[6]

Fase 3: Reageren (bevestigen ontvangst)

De LCI bevestigt de ontvangst van het verzoek (schriftelijk of digitaal) aan betrokkene. Hiervoor wordt door de projectgroep AVG een standaard tekst + afspraakvoorstel opgesteld. Kan de betrokkene niet worden geïdentificeerd of is dat nog niet gebeurd, dan wordt betrokkene gewezen op de mogelijkheid zich te identificeren bij het dichtstbijzijnde gerecht. Is aan de balie de identiteit met voldoende zekerheid vastgesteld, dan dient het verzoek in behandeling te worden genomen. Na het in behandeling nemen, kan de LCI de betrokkene verzoeken om aanvullende informatie te verstrekken ('preciseringsverzoek') als dat nodig is.

Een verzoekformulier wordt zodanig opgesteld dat betrokkene aan kan vinken wat voor hem/haar van toepassing is (hoedanigheid betrokkene, type procedure, bedrijfsvoering etc.).

Vreemde talen

Voorstel: Voor een verzoek in een andere taal dan de Nederlandse of Engelse gedaan, dient door betrokkene zelf een vertaling/tolk te worden geregeld. Het verzoek wordt in het Nederlands of Engels beantwoord. Dergelijke scenario's zullen vermoedelijk niet of slechts incidenteel voorkomen, zodat een algemene regel volstaat.

Mogelijkheden 'preciseringsverzoek':

- Aanduiding verzoek[7] (zie *Tabel A*).

[6] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/recht-op-inzage

[7] Het is denkbaar dat betrokkenen zekerheidshalve een verzoek indienen om uit te sluiten dat er persoonsgegevens van hen zijn, zonder dat een gerecht over die persoonsgegevens beschikt.

- Hoedanigheid van betrokkene: verdachte, slachtoffer, eiser, gedaagde, getuige(deskundige), advocaat, gemachtigde, rechter, personeelslid, curator, bewindvoerder, journalist, leverancier, minderjarige, onder curatele geplaatste.
- Ingeval het een rechtszaak / primair proces betreft of het gaat om:
    - Een lopende zaak, of een afgedane zaak (< 1, < 5 of langer dan 5 jaar geleden). Dit dient als aanknopingspunt voor de LCI om in te schatten waar het dossier/de gegevens zich bevinden.
    - Aard van de zaak en indien mogelijk het specifieke rechtsgebied civiel, bestuur, familie, kanton, straf, toezicht & bewind.
- Indien geen betrekking op rechtszaken informatie over aard van betrokkenheid zoals leveranciers, (oud)medewerkers, uitzendkrachten, abonnee op nieuwsbrieven etc.

Fase 4: Behandeling van verzoek

Wijze van behandeling

Een verzoek dient schriftelijk te worden afgehandeld. Volgens de AVG dient bij een digitaal ingediend verzoek *indien mogelijk* ook digitaal te worden beantwoord (art. 12 lid 3 AVG). Echter, binnen de Rechtspraak bestaat die mogelijkheid nog niet om per e-mail te antwoorden aangezien dit als niet veilig wordt beschouwd. Uitgangspunt is dus antwoorden op papier Behandeling van het verzoek is kosteloos, tenzij buitensporig vaak verzoeken worden ingediend. Het strekt te ver om hierover richtlijnen op te nemen, maar overleg met de CCI is raadzaam. De termijnen voor behandeling van een verzoek en de verlenging van die termijnen zijn in *Tabel B* opgenomen.

Opmerking: Hoewel op verzoek van betrokkene de verzochte informatie mondeling kan worden gegeven, op voorwaarde dat de betrokkene is geïdentificeerd (art. 12 lid 1 AVG), is het niet aan te bevelen verzoeken mondeling / telefonisch af te doen i.v.m. identificatie en vertrouwelijke en technische aard van de gegevens. Ook is dossieropbouw van belang voor het geval een betrokkene een klacht indient over de afhandeling van zijn verzoek. Voorts wordt in de externe communicatie opgeroepen het verzoek schriftelijk in te dienen en dat de Rechtspraak schriftelijk zal reageren.

a. Eenvoudige verzoeken

   Eenvoudige verzoeken kunnen met behulp van het verwerkingsregister worden afgehandeld op gerechtsniveau door de lokale coördinator informatieverzoeken zelf, eventueel met ondersteuning van de medewerkers van de verschillende rechtsgebieden (civiel, straf, bestuur, toezicht, familie, kanton etc.), de privacyfunctionaris van IVO en afstemming met de klachtenfunctionaris.

b. Complexe verzoeken

   Vragen naar aanleiding van complexere verzoeken kunnen in samenwerking met de collega's van de betreffende rechtsgebieden (straf, bestuur, civiel, etc.) worden beantwoord en indien nodig ter advies aan de CCI worden voorgelegd. Let op: wanneer blijkt dat het verzoek niet binnen één maand kan worden beantwoord, moet betrokkene daarvan op de hoogte gesteld worden **binnen de eerste maand**. Eveneens dient binnen die eerste maand verlenging van behandeltermijn aan betrokkene medegedeeld te worden (zie *bijlage B*). Een verzoek is in ieder geval complex indien het verzoek samenloopt met de reguliere inzageprocedures (art. 12 /30 -34 Sv, art. 7:18 lid 4 Awb (Wobverzoek, art. 843a Rv) / het een AVG-inzageverzoek betreft waarvan het vermoeden bestaat dat het bedoeld is om de reguliere inzageprocedure in een dossier te omzeilen. Denkbaar is dat betrokkene alle bovenstaande wegen, inclusief de AVG-weg, zal bewandelen om de informatie te verkrijgen. Bij een vermoeden van 'shoppen' (de betrokkene probeert via meerdere wegen aan bepaalde (proces)informatie te komen), is het aan te raden te communiceren met klachtenfunctionarissen, bestuurssecretarissen en behandelend rechters.

Verzoeken ten aanzien van persoonsgegevens in lopende strafdossiers/strafproces dienen te worden kortgesloten met het lokale parket/landelijk Openbaar Ministerie en de behandelend rechter, om te voorkomen dat lopend onderzoek wordt gefrustreerd.

c. Gerecht overstijgende /landelijke verzoeken
Verzoeken die gerecht overstijgend, landelijk of niet te herleiden zijn tot een specifiek gerecht kan men schriftelijk indienen bij de Raad voor de rechtspraak t.a.v. de coördinator informatieverzoeken. De CCI controleert bij IVO en/of het LDCR in welke systemen persoonsgegevens van verzoeker zijn geregistreerd en geeft die gegevens (samen met het verzoek) door aan het betreffende gerecht/gerechten met de vraag aan te geven of er nog lokale registraties zijn waarin persoonsgegevens van verzoeker zijn geregistreerd. Mocht dat het geval zijn dan worden die gemeld, waarna de CCI die de betrokkene informeert.

d. Inzage klachtdossier
Voor inzage in het klachtdossier geldt een ander reeds bestaand regime.

Ten slotte, bejegening en tevredenheid van de betrokkene zijn het uitgangspunt. Daarbij kan helpen dat - telefonisch - contact wordt opgenomen met de betrokkene en hij/zij wordt geholpen bij het verzoek. Waar is de betrokkene specifiek naar op zoek? Het is altijd goed om af te vragen welke informatie de betrokkene tevreden zou stellen en op zoek te gaan naar het achterliggende doel van het verzoek, om zo accuraat mogelijk antwoord te geven op het verzoek of de betrokkene door te verwijzen naar de juiste procedure.

Fase 5: Beantwoording van verzoek

Geen persoonsgegevens

Het kan zijn dat er geen persoonsgegevens zijn verwerkt van betrokkene.[8] Indien het verzoek betrekking heeft op één gerecht, laat de LCI weten dat betrokkene niet bekend is bij dat betreffende gerecht en dat er geen persoonsgegevens van hem of haar zijn verwerkt. Betreft het een verzoek dat meerdere gerechten aangaat, dan kan het antwoord dat geen persoonsgegevens zijn verwerkt alleen betrekking hebben op het specifieke gerecht. (Gerecht specifiek verzoek = gerecht specifiek antwoord, gerecht overstijgend verzoek = landelijk antwoord). Overigens is volgens de AVG een betrokkene elk natuurlijk persoon die direct of indirect kan worden geïdentificeerd.

Aan een verzoek wordt geen gevolg gegeven / het verzoek wordt beperkt

Slechts in zeer bijzondere situaties kan in zijn geheel dan wel beperkt geen gevolg worden gegeven aan een informatieverzoek. Het ‘niet kunnen vinden’ van gegevens kan daarom nooit als grond worden aangevoerd. Wanneer geen gevolg aan het verzoek gegeven kan worden, dient de betrokkene daarvan op de hoogte gebracht te worden. Het niet voldoen aan een verzoek dient gemotiveerd te zijn en te worden gearchiveerd (*zie Fase 6*).

Beperking van een verzoek is mogelijk indien dat op grond van een Europese of nationale wet is voorgeschreven dan wel door samenloop van nationale wetgeving (zoals Rv, Sv of de Awb) met de AVG, mits de beperking niet in strijd is met de inhoud van grondrechten en fundamentele vrijheden en een noodzakelijke en evenredige maatregel is (art. 23 AVG).

[8] Natuurlijke persoon die direct of indirect kan worden geïdentificeerd (artikel 4 sub 1 AVG).

Let op: Bij verzoeken t.a.v. het primaire proces is te verwachten dat eerder dan bij verzoeken t.a.v. bedrijfsvoering sprake is van een wet (EU/NL) of een samenloop van wetgeving op grond waarvan het verzoek niet ingewilligd of beperkt kan worden.

Verzoek wordt ingewilligd

Er zijn geen bezwaren op grond waarvan het verzoek van de betrokkene niet ingewilligd of beperkt zou moeten worden. Afhankelijk van het verzoek wordt op de volgende wijze aan het verzoek voldaan:

a. Intrekken toestemming verwerking persoonsgegeven
   Voor specifieke processen binnen de Rechtspraak die geen verband houden met het primaire proces kan het zijn dat de betrokkene toestemming heeft gegeven. Denk hierbij aan het versturen van een nieuwsbrief. Wanneer betrokkene de eerder gegeven toestemming intrekt, ontvalt de grond voor verwerking en dient de betrokkene uitgeschreven te worden.

b. Inzage persoonsgegevens
   Indien verzoeker heeft gevraagd om inzage in bijvoorbeeld het dossier van de procedure waarbij hij was betrokken beoordeelt de lokale coördinator informatieverzoeken, in overleg met betrokken rechter(s) of griffiemedewerkers, of aan het verzoek tot inzage persoonsgegevens kan worden voldaan. Soms volstaat het afgeven van een afschrift met daarin opgenomen welke persoonsgegevens in algemene zin worden verwerkt. Echter, de kans is groter dat betrokkene gewoon inzage wil in het volledig dossier. Wil betrokkene daadwerkelijk inzage op grond van de AVG, dan dient het dossier opgeschoond te worden aangezien vanuit de AVG **betrokkene slechts recht heeft op inzage voor zover het eigen persoonsgegevens betreft.** Persoonlijke aantekeningen van de combinatie evenals de interne correspondentie en het verslag in de Raadkamer dienen uit het dossier verwijderd te worden. Ook dienen de persoonsgegevens van anderen uit het dossier verwijderd te worden. Een verzoeker kan ook inzage vragen in zijn klachtdossier. Zeer persoonlijke aantekeningen (geheim van de raadkamer) van medewerkers van het gerecht mogen daaruit voor de inzage worden gehaald, maar over het algemeen moet dit dossier in principe integraal ter inzage worden gegeven, dus ook inclusief al het e-mailverkeer tussen medewerkers. De projectgroep beveelt aan om de correspondentie zakelijk te houden. De jurisprudentie op dit gebied is nog in ontwikkeling, maar op dit moment geldt dus kort gezegd: klachtdossier → volledige inzage en procesdossier → beperkte inzage. Het betreffende gerecht nodigt betrokkene uit en maakt een afspraak om betrokkenen de gelegenheid te geven het dossier in te zien. Betrokkene moet zich identificeren alvorens inzage te krijgen. Het is aan te bevelen om zoveel als mogelijk aan te sluiten bij de te volgen procedure van reguliere inzage en slechts inzage te verlenen in de aanwezigheid van een medewerker van het gerecht (bijv. griffier) om te voorkomen dat stukken uit het dossier worden verwijderd of gekopieerd.

   Inzage in digitale dossiers.
   PM.

c. Informatie over verwerking persoonsgegevens
   Het antwoord op het verzoek bevat ten minste (zie art. 15 lid 1 a-h AVG):
   - doeleinden van de verwerking;
   - categorie persoonsgegevens;
   - (categorie) van ontvangers;
   - bewaartermijnen;
   - dat de verzoeker het recht heeft te verzoeken gegevens te rectificeren of wissen en de verwerking te beperken of bezwaar te maken;
   - dat de verzoeker het recht heeft een klacht in te dienen bij de toezichthouder;

- wanneer de gegevens van een andere partij zijn verkregen, alle beschikbare informatie over deze bron;
- het bij de behandeling van dit informatieverzoek als zodanig persoonsgegevens zijn verwerkt.
- indien van toepassing, het bestaan van geautomatiseerde besluitvorming (incl. profilering) en nuttige informatie over de onderliggende logica, het belang en de verwachte gevolgen. In de regel heeft de rechtspraak hiermee overigens niet te maken.

d. Ontvangen kopie/afschrift persoonsgegevens
Een kopie van persoonsgegevens kan op verzoek worden verstrekt, indien de betrokkene kan worden geïdentificeerd en het recht om een kopie te verkrijgen geen afbreuk doet aan de rechten en vrijheden van anderen. Het is van belang om persoonsgegevens van anderen te anonimiseren, alvorens de kopieën te verstrekken. Het gaat hierbij dus niet om kopieën van hele dossiers. Voor zover processtukken reeds bekend zijn bij betrokkene, hoeft hiervan niet opnieuw een kopie te worden afgegeven.

e. Rectificatie: correctie / aanvulling persoonsgegevens
Onder correctie valt het verbeteren en/of aanvullen van persoonsgegevens. Correctie kan worden verzocht wanneer de persoonsgegevens feitelijk onjuist zijn, onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld en op een andere manier in strijd met de wet worden gebruikt. Rectificatie dient zonder onevenredige vertraging te geschieden (art 16 AVG).

f. Gegevenswissing: verwijdering van persoonsgegevens
Persoonsgegevens hoeven niet gewist te worden wanneer er sprake is van een wettelijke verplichting of een taak van algemeen belang en wanneer de gegevens nodig zijn voor de instelling, uitoefening of onderbouwing van een rechtsvordering (art. 17 lid 3 AVG). Aan dit soort verzoeken zal de Rechtspraak dus niet vaak gehoor kunnen geven. Wanneer een verzoek tot wissing gegrond is, dienen de partijen waarmee gegevens zijn gedeeld, op de hoogte gesteld te worden van het verzoek om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen. Verwijdering of afscherming van persoonsgegevens kan worden verzocht ingeval:
- De gegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld/verwerkt.
- Betrokkene zijn/haar eerder gegeven toestemming intrekt (zie onder a).
- Persoonsgegevens onrechtmatig zijn verwerkt.
- Persoonsgegevens moeten worden gewist o.g.v. de wet.

g. Beperking van verwerking persoonsgegevens
Beperking van verwerking (pauzeren) kan worden verzocht ingeval:
- de juistheid van de persoonsgegevens wordt betwist. Beperking geldt dan gedurende de periode die de verwerker in staat stelt de juistheid van de persoonsgegevens te controleren.
- De verwerking onrechtmatig is en betrokkene zich i.p.v. wissing beroept op beperking.
- De verwerker heeft de gegevens niet meer nodig, maar betrokkene heeft deze nodig voor instellen, uitoefenen of onderbouwen van rechtsvordering.
- Betrokkene heeft bezwaar gemaakt tegen verwerking (zie *Tabel D* sub 1).

h. Overdracht persoonsgegevens (dataportabiliteit)
De verwachting is dat een dergelijk verzoek binnen de Rechtspraak niet vaak zal voorkomen. Bovendien sluit artikel 20 lid 3 van de AVG het recht op gegevensoverdracht uit wanneer "… 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." Bij de Rechtspraak valt het merendeel van de verwerkingsprocessen binnen deze kaders, zodat aan een dataportabiliteitsverzoek niet voldaan hoeft te worden. Vanzelfsprekend dient de afwijzing te worden gemotiveerd.

Fase 6: Registratie & Archivering

De landelijke en lokale coördinatoren informatieverzoeken registreren de binnengekomen verzoeken zoals naam, adres, woonplaats, aard van het verzoek en wijze van afhandeling. (Zie Intro voor een template registratielijst). Op termijn zal *Demos* worden gebruikt om binnengekomen verzoeken per gerecht te registreren. Ook de doorlooptijd wordt vastgelegd. Het is aan te bevelen om eens per jaar met alle lokale coördinatoren informatieverzoeken ervaringen uit te wisselen en de knelpunten te bespreken om de eenduidigheid in de afhandeling te bevorderen. Dit zou kunnen door het opstellen van een lijst met meest gestelde vragen /meest voorkomende verzoeken.

Fase 7: Klachten

Als een betrokkene van mening is dat de verwerking door het gerecht of landelijke dienst van hem betreffende persoonsgegevens inbreuk maakt op de AVG of de krachtens de Richtlijn vastgestelde bepalingen, kan de betrokkene bij de volgende drie externe toezichthouders een klacht indienen.

Betrokkenen kunnen overigens er ook voor kiezen geen klacht in te dienen maar de Staat direct civielrechtelijk aansprakelijk te stellen door een aansprakelijkheidsstelling in te dienen bij het gerechtsbestuur. De LCI van het betreffende gerecht stelt de FG onverwijld in kennis van aansprakelijkstellingen.

I. De klachtenprocedure bij AP t.a.v. bedrijfsvoering

Betrokkenen hebben het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens als het gaat om persoonsgegevens die in het kader van de bedrijfsvoering worden verwerkt. Die procedures worden beschreven op Rechtspraak.nl. Wanneer betrokkene een klacht wil indienen die betrekking heeft op bejegening, volstaat een verwijzing naar de klachtenprocedure. In ieder geval heeft betrokkene het recht een klacht in te dienen wanneer zijn/haar verzoek m.b.t. persoonsgegevens niet in behandeling is genomen / afgewezen (zie *Tabel D*).

Klachten ten aanzien van de verwerking van persoonsgegevens in het kader van de uitoefening van gerechtelijke taken

II. De klachtenprocedure bij de Procureur-Generaal van de Hoge Raad
Voor de gerechten (rechtbanken, gerechtshoven en Hoge Raad) is dat toezicht belegd bij de procureur-generaal van de Hoge Raad.

De gerechten en het parket bij de Hoge Raad hebben er voor gekozen om het toezicht op de verwerking van persoonsgegevens in de rechtspraak toe te vertrouwen aan de door hen aangewezen functionarissen voor gegevensbescherming en de procureur-generaal bij de Hoge Raad. Dit is vastgelegd in de 'Regeling toezicht verwerking persoonsgegevens door gerechten en het parket bij de Hoge Raad' (zie <Link naar Regeling toezicht verwerking persoonsgegevens door gerechten en het parket bij de Hoge Raad>).

De toezichthoudende rol van de PG bestaat onder meer uit het behandelen van klachten van betrokkenen die van mening zijn dat de verwerking van hun persoonsgegevens door de gerechten of het parket bij de Hoge Raad inbreuk maakt op de AVG of de krachtens de richtlijn vastgestelde bepalingen. De PG zal jaarlijks, in het reguliere jaarverslag, verslag doen van zijn activiteiten en een

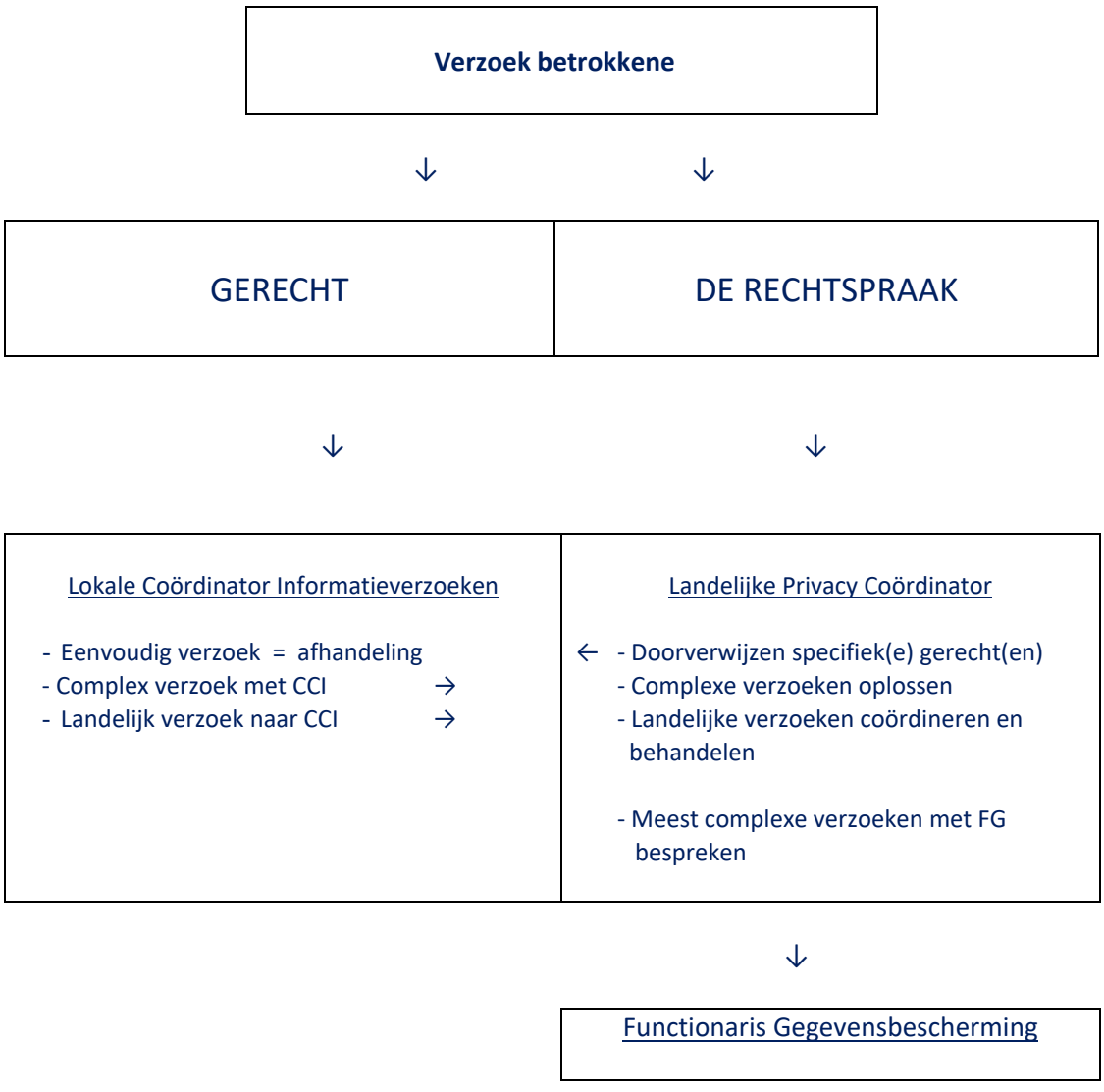
lijst publiceren van de soorten klachten, gemelde inbreuken en de eventueel ingestelde vorderingen bij de Hoge Raad.

III. De klachtenprocedure bij de “AVG-commissie bestuursrechtelijke colleges”

De toezichthoudende rol van de PG betreft niet het toezicht op de verwerking van persoonsgegevens door de bestuursrechtelijke colleges. Voor de bestuursrechtelijke colleges (Afdeling bestuursrechtspraak Raad van State, Centrale Raad van Beroep en het College van Beroep voor het bedrijfsleven) is het toezicht belegd bij de nieuw ingestelde “AVG-commissie bestuursrechtelijke colleges”. Daarvoor geldt de volgende regeling: (zie <Link> op www.rechtspraak.nl).

Bijlagen – Beslisboom & Overzicht van Tabellen

Beslisboom



Tabel A: Overzicht mogelijke AVG-verzoeken

	Verzoek type	**Artikel AVG**
1.	Intrekken toestemming verwerking persoonsgegevens	Art. 7 lid 3 AVG
2.	Inzage persoonsgegevens	Art. 15 lid 1 AVG
3.	Informatie over verwerking persoonsgegevens	Art. 15 lid 1 AVG
4.	Ontvangen kopie persoonsgegevens	Art. 15 lid 3 AVG
5.	Rectificatie: correctie / aanvulling persoonsgegevens	Art. 16 AVG
6.	Gegevenswissing: verwijdering van persoonsgegevens	Art. 17 AVG
7.	Beperking van verwerking persoonsgegevens	Art. 18 AVG
8.	Overdracht persoonsgegevens (dataportabiliteit)	Art. 20 AVG

Tabel B: Termijnen van behandeling

1.	**Eenvoudige verzoeken** *1 maand*	Eenvoudige verzoeken worden zo snel mogelijk, maar uiterlijk binnen één maand afgehandeld.	Art. 12 lid 3 AVG
2.	**Complexe verzoeken** *3 maanden (1+2 maanden)*	Voor complexe verzoeken kan de termijn van één maand worden verlengd met nog twee maanden, mits dat is medegedeeld aan de betrokkene binnen de eerste maand na ontvangen verzoek.	Art. 12 lid 3 AVG
3.	**Geen gevolg geven aan verzoek** *1 maand*	Binnen 1 maand, wijzen op klachtprocedure + redenen geen gevolg geven.	Art. 12 lid 4 AVG

Tabel C: redenen beperken / geen gevolg geven aan verzoek

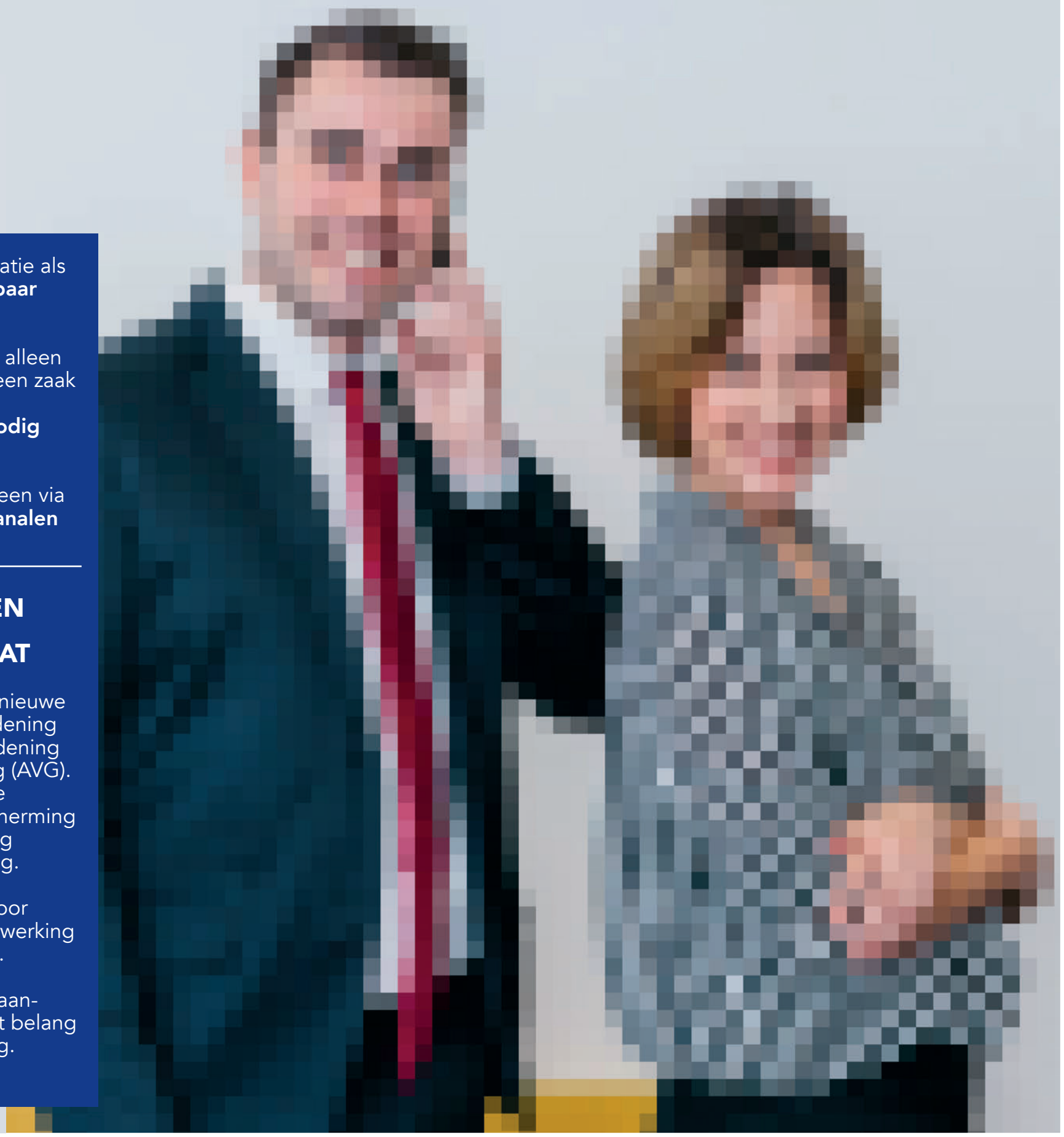
	Geen gevolg geven aan verzoek	Aan een verzoek kan geen gevolg worden gegeven. Opgave van de reden(en) tot afwijzing is verplicht. Tevens dient gewezen te worden op de mogelijkheid tot het indienen van een klacht (klachtenprocedure) of beroep bij de bestuurs- of civiele rechter.	Art. 12 lid 4 AVG
1.		De verordening niet van toepassing is omdat: - gegevens worden verwerkt met het oog op voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten. - de tenuitvoerlegging van straffen. - bescherming tegen en voorkoming van gevaren openbare veiligheid/nationale veiligheid. - Rechten en vrijheden van anderen dienen te worden beschermd.	Art. 1 lid 2 sub d AVG
2.		Nadat aanvullende gegevens zijn gevraagd, is identificatie van betrokkene nog steeds niet mogelijk.	Art. 11 lid 2 jo Art. 12 lid 2 AVG
3.		Buitensporige verzoeken (repetitief).	Art. 12 lid 5 AVG
	Beperken rechten betrokkene	Wettelijke grondslag maakt beperking van verzoek mogelijk, mits die beperking grondrechten en fundamentele vrijheden onverlet laat en noodzakelijk en evenredig is ter waarborging van:	Art 23 AVG
		a. De nationale veiligheid; b. Landsverdediging; c. Openbare veiligheid; d. Voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, incl. bescherming en voorkoming van gevaren voor openbare veiligheid; e. Doelstellingen van de EU of van een lidstaat (economisch/financieel, monetair, budgettair, fiscaal, volksgezondheid en sociale zekerheid); f. 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; h. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van openbaar gezag in de bovengenoemde gevallen (m.u.v. punt f.); i. Bescherming van betrokkene of rechten en vrijheden van anderen; j. Inning van civielrechtelijke vorderingen.	

Tabel D: Mogelijkheden klachten

1.	Geen gevolg geven aan verzoek onder A.	
2.	Klacht t.a.v. de inhoud van verzoek onder A.	
3.	Klacht t.a.v. afwikkeling verzoek.	

Document 9:
Poster ga zorgvuldig om met persoonsgegevens

Ga zorgvuldig om met persoonsgegevens



- Verstrek alleen informatie als mensen het **aantoonbaar mogen ontvangen**
- Bekijk **processtukken** alleen voor het werken aan een zaak
- **Bewaar alleen wat nodig** of verplicht is
- Verstuur gegevens alleen via **veilige rechtspraakkanalen**

BESPREEK BINNEN JE TEAM HOE JE HIER MEE OMGAAT

Vanaf 25 mei gaat een nieuwe Europese privacyverordening in, de Algemene Verordening Gegevensbescherming (AVG). Voor het strafrecht is de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn) van toepassing.

De Rechtspraak gaat door met de zorgvuldige verwerking van persoonsgegevens. De nieuwe regelgeving betekent dat we vaker aandacht besteden aan het belang van privacybescherming.

JIJ BENT DE SLEUTEL

Check de intropagina voor meer informatie
Intro Landelijk/Bedrijfsvoering/Beveiliging/Jij-bent-de-sleutel/
en **Intro Landelijk/Projecten/Privacywetgeving AVG Richtlijn**

de Rechtspraak

Document 10:
Drie speerpunten en 10 gouden privacyregels

de Rechtspraak

Drie speerpunten en 10 gouden privacyregels

1. Toegang (jij bent de sleutel)

1.1 Beperk autorisatie medewerkers tot noodzaak.

1.2 Let op clean desk policy, gesloten ruimten en kasten.

1.3 Let op e-mail en internet gebruik, USB-sticks, thuiswerken.

2. Verstrekking

Verstrek alleen gegevens na:

2.1 Vaststelling wettelijke grondslag.

2.2 Vaststelling identiteit van de betrokkene.

2.3 Vaststelling bevoegdheid verzoeker.

En:

2.4 Bescherm privacy anderen in dossiers en registraties.

3. Registreren en bewaren

3.1 Verwerk niet meer dan nodig.

3.2 Bewaar niet langer dan nodig, vernietig als kan.

3.3 Beperk herleidbaarheid tot individu: door gegevens (NAW) uit een bestand te verwijderen, door anonimiseren.