Deelbesluit 10 - Datalekken
Document 341

KPI aandachtsgebieden Privacy Rechtspraak

Versie 23 september 2020

Inhoud

1. Inleiding

Met dit document wordt richting het ministerie gerapporteerd over de mate waarin de Rechtspraak voldoet aan de wet- en regelgeving t.a.v. privacy. Hierbij gaat het niet alleen om de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG), maar ook aan de verplichtingen die voortvloeien uit de Wet justitiële en strafvorderlijke gegevens (Wjsg) en het bijbehorende besluit.

Dit plan is ingedeeld conform de privacy management KPI's van JenV. In de tekst wordt steeds kort aangegeven waar de Rechtspraak staat en welke ambitie de Rechtspraak heeft ten aanzien van de betreffende KPI onderneemt. Per KPI wordt een kwaliteitsniveau en ambitieniveau bepaald

Bij de opbouw en de scoring van de KPI's moet worden opgemerkt dat het hier nog om een pilot gaat die uitgezet is binnen het Ministerie van Justitie en Veiligheid. De kwaliteits- en ambitieniveaus moeten nog bestuurlijk worden vastgesteld. Het gesprek hierover vindt plaats, zodra de pilotfase is afgerond en de KPI's formeel door het ministerie zijn vastgesteld. Tot die tijd worden de KPI's als indicatie gebruikt.

De beoordeling vindt plaats aan de hand van cijfers op een schaal van 1 tot en met 5, waarbij het getal 1 het laagst is en getal 5 het hoogst is. Hierbij moet worden opgemerkt dat het nadrukkelijk niet de bedoeling is om voor alle KPI's te streven naar het cijfer 5; er moet gekeken worden naar het ambitieniveau dat past bij de organisatie in de nabije toekomst, zo ook de Rechtspraak. Iedere organisatie kan op deze wijze een ontwikkeling doormaken v.w.b. privacy.

2. Privacy administratie

<table>
<tr><td colspan="4">De Privacy Administratie omvat alle aandachtsgebieden voor de verwerkingsverantwoordelijke (daarmee veelal de organisatie duidend) die een rol spelen bij het kunnen aantonen van en verantwoorden over de naleving c.q. het compliant werken aan van privacy wet- en regelgeving (Verantwoordingsplicht).

De KPI Privacy Administratie geeft de verwerkingsverantwoordelijke inzicht in de status quo van de wettelijk verplichte documentatieopbouw voor deze aandachtsgebieden (Documentatieplicht) en laat naar buiten zien wat er zoal op de rit is als onderbouwing voor de door de organisatie gehanteerde zorgvuldigheid in haar omgangsvormen met persoonsgegevens.</td></tr>
<tr><td>Kritieke Prestatie Indicator</td><td colspan="3">Privacy Administratie</td></tr>
<tr><td>Organisatie score</td><td>Niveau</td><td>Proceskwaliteit</td><td>Gerealiseerd</td></tr>
<tr><td></td><td>5</td><td>Geoptimaliseerd</td><td>1. Er is centraal inzicht in (de status van) alle verwerkingen in het register van verwerkingen mogelijk door de FG, waarmee diens adviestaak (art. 35.2) wordt ondersteund. Bewaking op de naleving van maatregelen om tekortkomingen te mitigeren wordt (geautomatiseerd) gestructureerd ondersteund.
2. Er is centraal inzicht in (de status van, waaronder daarbij onder handen zijnde (herijkings)assessments in het kader van de Privacy Management Control Cyclus) voor alle DPIA’s mogelijk voor de FG, waarmee diens adviestaak (art. 35.2) wordt ondersteund.
3. De organisatie beschikt over een toestemmingadministratie waaruit te allen tijde kan worden afgeleid wanneer en waarvoor toestemming is gegeven alsmede is ingetrokken. De relatie kan worden gelegd tot op de verwerkingsgerichte handeling waar de toestemming op van toepassing is.
4. Er is een workflow ingericht die de achtergronden van informatiebeveiligingsincidenten bij de bron (de melder) documenteert (en waar mogelijk direct mitigeert), de analyse hiervan (wel/geen (meldenswaardig) datalek) vormgeeft en de beschikbare tijd (max 72 klokuren) zo volledig mogelijk beschikbaar maakt voor de operationele afhandeling van datalekken.
5. Privacy beleid wordt periodiek en structureel binnen de Privacy Management Control Cyclus op de beoogde werking (instrueren van medewerkers omtrent de omgang met persoonsgegevens) herijkt en waar van toepassing aangepast en/of geactualiseerd.
6. Betrokkenen worden op gestructureerde wijze geïnformeerd omtrent het verwerken van hun persoonsgegevens vóórdat er sprake van verwerken is.</td></tr>
</table>

4	4	Voorspelbaar	1. Het register van verwerkingsactiviteiten kent een nadere onderbouwing van elke verwerking. Op basis hiervan kan de kwaliteit van verwerkingen kan worden bewaakt en kan hierover op elk gewenst inhoudelijk niveau worden gerapporteerd. Het register van verwerkingsactiviteiten biedt hiermee tevens inzicht in de kwalitatieve ontwikkeling van verwerkingen in de tijd (periodieke herijkingen). Logging maakt onderdeel uit van de aandacht van de verwerkingsverantwoordelijke, om desgevraagd de handelingen die met persoonsgegevens zijn verricht tot op een diepgang die de AVG vereist (zie NEN 7513 als goed voorbeeld van een gedegen uitwerking hiervoor), te kunnen verantwoorden. 2. De risicoafweging van DPIA's worden gestructureerd en op eenduidige wijze gedocumenteerd. De naleving van het als actie benoemen, agenderen en door voeren van gesignaleerde verbeteringen, wordt bewaakt. De herhaalbaarheid van assessments is groot. Periodiek rapporteren aan management kan (geautomatiseerd) op eenvoudige wijze worden vormgegeven. 3. Er is een centrale registratie van toestemming en de status hiervan kan te allen tijde op verwerkingenniveau worden getoond. 4. Er is een duidelijk en binnen de organisatie geborgd protocol voor de afhandeling van datalekken. Uit de registratie van informatiebeveiligingsincidenten wordt periodiek lering getrokken. Verworven inzichten worden gebruikt in opleidingen voor medewerkers, bijvoorbeeld om dergelijke incidenten in de toekomst waar mogelijk te voorkomen (privacy bewustzijn vergroten) en bij de ontwikkeling van nieuwe (werk)processen, informatie-systemen, beleid en wetgeving. 5. Privacy beleid wordt actief uitgedragen binnen de organisatie, onder andere in opleidingen. 6. De publicatie van een privacyverklaring op internet is aangevuld met situationeel in te zetten informatiemateriaal. Dit materiaal dient om betrokkenen, zodra zij een raakvlak krijgen in een betreffende situatie, op correcte en gestructureerde wijze te informeren omtrent het verwerken van zijn/haar persoonsgegevens en de achtergronden daarvan.
5	3	Vastgesteld	1. Het stramien van documenteren van verwerkingen in het register van verwerkingsactiviteiten vergroot de herhaalbaarheid (het herijken). Bovendien maakt het de daartoe vereiste effort (beslag op resources) acceptabel. Hierbij wordt doorontwikkeld aan het gestructureerd en geformaliseerd afhandelen van onderkende tekortkomingen en risico's voor de aandachtsgebieden van AVG art. 30 ergo het compliant werken en kunnen komen tot een verantwoorde maatregelenmix en bewaking van de naleving daarvan. 2. Het documenteren van DPIA's is omgeven met een workflow waarvan de beoordeling (kwaliteit/QA en juridisch) ervan een vast onderdeel uitmaakt. Het beoordelingsresultaat is opgenomen in de documentatie. 3. Verkrijgen en intrekken van toestemming bij verwerkingen wordt waar dit speelt eenduidig vastgelegd. Er wordt op

			toegezien dat al naar gelang op correcte wijze wordt gehandeld, zoals de verwerking waar toestemming voor nodig was maar die ingetrokken is, staken en daarbij vereiste handelingen verrichten (zoals bijvoorbeeld wissen). 4. Het centraal ondersteunen van incidentenregistratie, beoordeling, kwalificatie en afhandeling (waaronder datalekken) begint vorm te krijgen. 5. Er is een gestructureerd Privacy beleid dat door MT is vastgesteld. Dit beleid wordt actief uitgedragen naar personeel/medewerkers, onder meer via opleidingen. 6. Er is een privacyverklaring beschikbaar. Er wordt gewerkt aan procedures om de informatieplicht nader vorm te geven bij situationele verwerkingen.
2, 3, 6	2	Beheerst	1. Er worden lokaal binnen de organisatie handmatig beheerde registraties van verwerkingen bijgehouden conform de AVG art.30 vereisten. De organisatie werkt aan een centrale registratie hiervoor. Bijkomend doel is lokale initiatieven voor dergelijke vastleggingen - waar van toepassing - te kunnen beëindigen. 2. Er wordt op gestructureerde wijze vormgegeven aan het opstellen en beheren van DPIA's op papier, uitgevoerd conform het Model Gegevensbeschermingseffect-beoordeling rijksdienst (PIA). 3. Gegeven toestemming wordt op procesniveau dus situationeel gedocumenteerd, evenals het eventueel weer intrekken hiervan. 4. Er is een situationele datalekkenprocedure. De beoordeling en afhandeling van informatiebeveiligingsincidenten worden ad hoc gevolgd. 5. Privacy beleid bestaat nog niet maar is inmiddels in ontwikkeling. 6. Een privacyverklaring is extern beschikbaar.
1	1	Informeel	1. De verwerkingsverantwoordelijke verkeerd nog in de fase van ontdekken hoe efficiënt en effectief vorm te geven aan haar documentatieverplichtingen. De organisatie is hiertoe bezig zijn privacy verplichtingen uit te werken qua context en inhoud alsmede beheerbenadering. Er is op lokaal niveau lokaal een basale vastlegging van verwerkingen aan het ontstaan. 2. DPIA's c.q. risicoassessments worden ad hoc en situationeel op papier uitgevoerd conform het Model Gegevensbeschermingseffectbeoordeling rijksdienst (PIA). 3. Toestemming wordt impliciet aanwezig geacht indien persoonsgegevens worden verwerkt. Er vindt geen registratie van plaats. 4. Registratie en het volgen van informatiebeveiligingsincidenten alsmede de analyse of dit datalekken betreft wordt ad hoc en situationeel (waar het zich voordoet) geregeld. 5. Privacy beleid ontbreekt. 6. Er wordt gewerkt aan een centrale privacyverklaring voor de organisatie.

Onderbouwing score Privacy administratie	
1 Register van verwerkingsactiviteiten	
Onderbouwing kwaliteitsniveau:	Voorafgaand aan de inwerkingtreding van de AVG is door de projectleiding van het AVG-project van het Bureau Rvdr een landelijk verwerkingsregister opgesteld. In dat kader is gerealiseerd in samenwerking met IVO, gerechten en diensten: ✓ Landelijk register: 150+ IT applicaties (beheer IVO); ✓ Lokale registers: lokale IT en registraties (beheer gerechten en landelijke diensten zelf).
Ambitieniveau:	De Rechtspraak heeft (nog) niet de ambitie om een centrale structuur op te zetten voor alle registers van verwerkingsactiviteiten. Ieder gerecht is hier immers zelf verantwoordelijk voor.
2 DPIA's	
Onderbouwing kwaliteitsniveau:	PIA's worden uitgevoerd conform het Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) dat is aangepast aan de Rechtspraak. Daarnaast wordt in sommige gevallen gebruik gemaakt van de PIA Light.
Ambitieniveau:	De aanschaf van de PIA-tool zorgt ervoor dat het uitvoeren van PIA's eenvoudiger wordt en dat er een automatische workflow op basis van de PDCA-cyclus ontstaat.
3 Toestemmingsregister	
Onderbouwing kwaliteitsniveau:	De verwerkingen van de Rechtspraak worden grotendeels gebaseerd op de grondslagen: wettelijke verplichting (art. 6, lid 1, sub c AVG) en de taak van algemeen belang (art. 6, lid 1 sub e AVG). In gevallen dat toestemming als grondslag wordt gebruikt, vindt documentatie daarvan plaats. Voor wat betreft de Wjsg is dit een wettelijke verplichting.
Ambitieniveau:	Voor de Rechtspraak is het van belang dat voor ieder gerecht en voor iedere landelijke dienst te allen tijde duidelijk is bij welke verwerkingen de grondslag toestemming wordt gebruikt en dat het proces hieromtrent vastgelegd en geborgd is. Door de FG wordt hierop toegezien.
4 Datalekregister	
Onderbouwing kwaliteitsniveau:	De procedure voor het melden van datalekken is van kracht sinds de zomer van 2016. In oktober 2019 is deze procedure vernieuwd in het handboek datalekken. De beveiligings- en privacy coördinatoren bij gerechten en diensten zijn verantwoordelijk voor de uitvoering van de procedure.
Ambitieniveau:	Door het Landelijk Overleg Beveiligingscoördinatoren Rechterlijke Organisatie worden interne afspraken gemaakt over de juiste interpretatie en uitvoering van de datalekregels ter voorkoming van onjuist uitkomsten. Hierbij valt de denken aan de inschatting van het risico.
5 Gegevensbeschermingsbeleid	
Onderbouwing kwaliteitsniveau:	Het gegevensbeschermingsbeleid wordt binnen de Rechtspraak in meerdere documenten op meerdere niveaus vormgegeven. Het beleid wordt periodiek herijkt op basis van de PDCA-cyclus.
Ambitieniveau	Verbeteringen zijn gelegen in het meer actief uitdragen van het privacybeleid door de besturen en directies en het faciliteren van opleidingen. Dit laatste wordt inmiddels ook in kaart gebracht door de werkgroep bewustwording.

6 Privacyverklaring	
Onderbouwing kwaliteitsniveau:	Door de Rechtspraak is de algemene privacyverklaring gepubliceerd op rechtspraak.nl. De informatie hierin is uitgesplitst per rechtsgebied. Daarnaast is onlangs op de vacaturepagina van de Rechtspraak een aparte privacyverklaring gepubliceerd.
Ambitieniveau:	De Rechtspraak moet meer grip krijgen op gegevensverwerkingen die naast het primaire proces plaatsvinden, zoals het wervings- en selectietraject. Hierna kan de informatieplicht hierop worden aangepast.

3. Transparantie

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

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

Kritieke Prestatie Indicator	**Transparantie**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
3	5	Geoptimaliseerd	1. Reacties van betrokkenen wordt gestructureerd meegenomen bij het opstellen, herijken, beheer en onderhoud van de communicatie en het informeren van betrokkenen over de verwerking van persoonsgegevens. 2. Betrokken worden altijd geïnformeerd over het verwerken van persoonsgegevens voordat dit plaatsvindt. 3. Betrokkenen kunnen informatie over verwerkingen eenvoudig vinden en worden geholpen om hun vragen daaromtrent te stellen.
	4	Voorspelbaar	1. Periodiek vindt binnen de Privacy Management Control Cyclus verificatie en toetsing plaats van de ingerichte werkwijze en procedures om betrokkenen passend te informeren omtrent (de achtergronden van) verwerkingen. 2. Het tijdig en adequaat informeren van betrokkenen omtrent verwerkingen maakt integraal onderdeel uit van de Privacy Management Control Cyclus. 3. Er is een (online) procedure ingericht voor betrokkenen bij verwerkingen om hun privacy rechten op eenvoudige wijze uit te kunnen oefenen.
1, 2	3	Vastgesteld	1. Het informeren van betrokkenen over verwerkingen en welke informatie daarbij wordt verwerkt is eenduidig, formeel en procesmatig vastgelegd. Er is consistentie in de uitvoering. 2. De organisatie beschikt over een privacyverklaring waarmee alle informatie omtrent verwerken door de organisatie namens de verwerkersverantwoordelijke voor betrokkenen op één plaats wordt aangeboden. Er kan eenvoudig nadere inhoudelijke informatie bij en over specifieke verwerkingen aan betrokkenen worden verstrekt. 3. Er zijn - waar proces technisch mogelijk - flyers of anderszins voorzieningen gecreëerd om betrokkenen vooraf te informeren omtrent het verwerken van persoonsgegevens op een zo begrijpelijk mogelijke manier (bijvoorbeeld in meer talen beschikbaar).

	2	Beheerst	1. Binnen de organisatie is vastgelegd wanneer en hoe betrokkenen vooraf worden geïnformeerd en welke informatie wordt verstrekt. 2. Er is duidelijk welke informatie verstrekt moet worden in het kader van de informatieplicht en er wordt gewerkt aan een manier om betrokkenen dit ook aan te reiken. 3. Er wordt gewerkt aan informatiemateriaal dat gebruikt kan worden om betrokkenen te informeren omtrent het verwerken van persoonsgegevens.
	1	Informeel	1. Er wordt gewerkt aan werkvormen voor het informeren van betrokkenen omtrent het verwerken van persoonsgegevens. 2. Of en hoe betrokkene wordt geïnformeerd en welke informatie wordt verstrekt is situationeel en sterk afhankelijk van keuze (en kennis op dit vlak) van de lijnverantwoordelijke binnen de organisatie. 3. Betrokkenen worden situationeel en ad hoc geïnformeerd omtrent verwerkingen. Het behandelen van een verzoek tot het uitoefenen van een of meer rechten van betrokken vindt op gelijksoortige wijze plaats.

Onderbouwing score transparantie	
1 Inhoud informatie	
Onderbouwing kwaliteitsniveau:	Op rechtspraak.nl/privacy worden de 5w- en h- vragen beantwoord onder de veelgestelde vragen. Verder gelden voor de bewaartermijnen van documenten in het primaire proces de basisselectiedocumenten. Deze zijn gepubliceerd op nationaalarchief.nl
Ambitieniveau:	Met de aanschaf van de PIA tool ontstaat een meer structureel proces om privacy te borgen. Dit zal er ook voor zorgen dat de gepubliceerde informatie op basis van de PDCA-cyclus steeds zal worden bijgewerkt.
2 Toegankelijkheid informatie	
Onderbouwing kwaliteitsniveau:	Uit aandachtspunt 6 van de KPI Privacy Administratie is gebleken dat de Rechtspraak op twee verschillende plekken een privacyverklaring heeft gepubliceerd: een algemene op rechtspraak.nl en een verklaring die aansluit bij de sollicitatieprocedure van de Rechtspraak. Mochten betrokkenen geïnteresseerd zijn in meer informatie over de Rechtspraak dan kunnen ze gebruikmaken van de verschillende communicatiekanalen die de Rechtspraak aanbiedt, zoals Facebook, Twitter, Instagram en Whatsapp.
Ambitieniveau:	Net als bij het vorige aandachtspunt zal de privacyverklaring door de nieuwe PIA-tooling continu geüpdatet worden op basis van de behoefte van betrokkenen.
3 Faciliteren uitoefenen privacy rechten door betrokkenen	
Onderbouwing kwaliteitsniveau:	De procedure voor het beantwoorden van informatieverzoeken van betrokkenen is gepubliceerd op rechtspraak.nl/privacy en op Intro voor interne betrokkenen. De procedures zijn ingevoerd binnen de Rechtspraak.
Ambitieniveau:	Er zijn geen signalen dat er op dit punt op korte termijn nog acties ondernomen dienen te worden.

4. Privacy by design (PbD) en Default

De KPI PbD geeft de verwerkingsverantwoordelijke voor zijn organisatie inzicht in de mate waarin rekening wordt gehouden met het kwaliteitsaspect privacy als aandachtspunt bij het ontwikkelen van nieuwe (werk)processen, informatiesystemen en/of beleid of wetgeving. De focus van de KPI PbD ligt daarmee bij het borgen van de belangenbescherming van de betrokkene waar persoonsgegevens van worden verwerkt.			
Kritieke Prestatie Indicator	**Privacy by Design/Default (PbD)**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	1. Voor nieuwe (of vernieuwde c.q. van een grote release voorziene) informatiesystemen, werkprocessen of wetgevingstrajecten is het principe van Privacy by Design en Default doorgevoerd in de maatregelenmix. Het bewaken van de implementatie van deze principes is geborgd binnen de Privacy Management Control Cyclus (op een voor de verwerkingsverantwoordelijke passend niveau) door registratie van de gedurende de ontwikkeling gemaakte privacy afwegingen in het register van verwerkingsactiviteiten. 2. Uit het register van verwerkingsactiviteiten zijn naast de verkozen maatregelenmix tevens de gemaakte afwegingen om tot een oplossingsrichting te komen af te leiden. 3. Voor verwerkingen waarbij keuzeafwegingen moeten worden gemaakt met een mogelijke impact op de persoonlijke levenssfeer van betrokkenen wordt bij het invullen altijd standaard de optie die de minste impact heeft op de betrokkene geselecteerd of er zijn organisatorische waarborgen ingesteld om dit te borgen.
	4	Voorspelbaar	1. Nieuwe verwerkingen worden alleen operationeel doorgevoerd (decharge) als aan alle privacy verplichtingen is voldaan gekenmerkt door aantoonbaarheid vanuit de Privacy Administratie. Dit omvat de maatregelenmix in het kader van Privacy by Design gedurende de ontwikkelfase periodiek geëvalueerd en getoetst is aan de stand der techniek (wat is er mogelijk) en uitvoeringskosten (wat kost dat) afgezet tegen de risico's die met de verwerking gepaard gaat en de aard van de te beschermen persoonsgegevens. 2. In de beschouwing van passende bescherming van persoonsgegevens bij verwerkingen wordt het belang van betrokkenen primair gesteld. Bij selectietrajecten om oplossingen te verwerven is het hier niet aan voldoen een showstopper voor de oplossingsvariant. 3. Er is gestructureerd aandacht voor het belang van bescherming van de persoonlijke levenssfeer van betrokkenen bij verwerkingen.
	3	Vastgesteld	1. Gedurende de gehele looptijd van een project/verwerking wordt periodiek de bescherming van persoonsgegevens gevalideerd voor de oplossingsrichting en daaruit ontleende oplossingsvariant. Deze activiteit wordt gedocumenteerd (aantoonbaar) in het register van verwerkingsactiviteiten op een zodanige wijze dat in het ontwerp van verwerkingen de bescherming van de persoonlijke levenssfeer van betrokkenen op een voor de verwerkingsverantwoordelijke passend niveau is verankerd.

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

Onderbouwing score privacy by design/default (PdD	
1 Privacy wordt meegenomen in ontwerpfase	
Onderbouwing kwaliteitsniveau:	De meeste IT- ontwikkelingen vinden plaats bij IVO Rechtspraak. Verder wordt bij IVO privacy by design geïmplementeerd in de ontwikkelprocedures. Bij steeds meer ontwikkelingen wordt privacy by design gebruikt, maar een structurele aanpakt waarbij privacy daadwerkelijk vanaf het begin betrokken is, is nog in ontwikkeling. Voor zover er lokale ontwikkelingen zijn, zal privacy ad hoc aandacht krijgen in de ontwerpfase. Het principe van PbD is bij de gerechten onvoldoende bekend. Desalniettemin betekent dit niet dat er (grote) steken vallen. Diensten en IT-producten worden via de inkoopafdeling van het LDCR of IVO aangeschaft. Bij deze inkoopafdelingen zijn procedures ontwikkeld om privacy te borgen door een PIA uit te voeren en, voor zover nodig, door verwerkersovereenkomsten af te sluiten.
Ambitieniveau:	De Rechtspraak beoogt privacy by design verder te implementeren bij IVO Rechtspraak. Voorts zullen de gerechten ondersteund worden in de toepassing van privacy by design bij lokale initiatieven waarbij persoonsgegevens worden verwerkt.
2 Afwegingen in het kader van beoordeling passende maatregelen	
Onderbouwing kwaliteitsniveau:	Bij het merendeel van de verwerkingen zijn de maatregelen in kaart gebracht en geïmplementeerd. Er is echter nog werk dat opgepakt en gestructureerd moet worden uitgevoerd.
Ambitieniveau:	Zoals uit de bespreking hierboven blijkt, is de Rechtspraak goed op weg om de privacy structureel in de organisatie te borgen. Met de acties die de Rechtspraak uitvoert en nog wil gaan uitvoeren, sluit zij aan bij de voorbeeldfunctie die de Rechtspraak in de maatschappij heeft.
3 Privacy by default	
Onderbouwing kwaliteitsniveau:	Het privacybewustzijn neemt steeds verder toe en medewerkers stellen steeds vaker vragen waarmee qua privacy rekening gehouden moet worden. Aan de andere kant gebeurt er ook nog veel onder de radar. Bij grote of langdurige (IT-)projecten wordt een PIA uitgevoerd en steeds de vraag gesteld of een verwerking met minder gegevens kan plaatsvinden. Veelal wordt hier aan voldaan.
Ambitieniveau:	De Rechtspraak beoogt het bewustwordingsniveau verder te vergroten en privacy by default structureel te borgen. De eerste stap is de PIA-tool, zodat PIA's eenvoudiger kunnen worden uitgevoerd. Daarna kan het privacyproces verder geborgd worden.

5. Betrokken partijen

De KPI Betrokken partijen geeft inzicht in de wijze waarop organisatiegrens overschrijdend verkeer van persoonsgegevens is ingeregeld en persoonsgegevens buiten de beheersfeer van de verwerkingsverantwoordelijke en daarmee de organisatie raken. Deze KPI kijkt op persoonsgegevensstromen van en naar betrokken partijen in verwerkingen. De onderbouwing van de rechtmatigheid van dit verwerken is een aspect waar de verwerkingsverantwoordelijke zich over dient uit te spreken en zijn maatregelenmix op moet inregelen. Documenteren hiervan vindt plaats in het register van verwerkingsactiviteiten conform en langs de vereisten van AVG art. 30.			
Kritieke Prestatie Indicator	**Betrokken partijen**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	1. De afsprakenkaders voor het verwerken van persoonsgegevens zijn voor elke verwerking die hiervoor in aanmerking komt tussen de partijen afgestemd en op passende wijze aantoonbaar gedocumenteerd en actueel. 2. Bij delen van persoonsgegevens buiten de organisatiegrenzen worden de onderlinge verhoudingen (verwerkingsverantwoordelijke, verwerker, gezamenlijk verwerkingsverantwoordelijk) periodiek (binnen de Privacy Management Control Cyclus van 3 jaar) herijkt. 3. Er is een duidelijk kader en/of richtlijnen en vastgelegde structuur voor levering van persoonsgegevens met derde landen beschikbaar, die het vereiste beschermingsniveau van persoonsgegevens hierbij borgt. 4. Het hoger management stuurt op het volgens beleid correct verwerken van persoonsgegevens en monitort daarbij de naleving van de belangen van betrokkenen.
1, 3	4	Voorspelbaar	1. De afsprakenkaders tussen partijen zijn helder, effectief en efficiënt vastgelegd in daartoe geëigende en met elkaar vastgestelde formele documenten. 2. De onderlinge verhoudingen tussen de partijen is eenduidig met elkaar overeengekomen en gedocumenteerd. 3. Er is bij internationale doorgifte structureel aandacht voor het belang van de impact van adequaatheidsbeslissingen op de (on)rechtmatigheid van verwerkingen. Er vindt sturing plaats op de toepassing van het centraal bepaalde beleid m.b.t. vastlegging en vaststelling van de grond van de verder verwerking. 4. De wijze waarop invulling gegeven wordt aan de rechten van betrokkenen en het informeren over verwerkingen van betrokken is vastgelegd in processen.
2, 4	3	Vastgesteld	1. Er is duidelijk hoe verantwoordelijkheden liggen; eenzijdige verwerkingsverantwoordelijkheid, gezamenlijke verwerkingsverantwoordelijkheid, verwerker. 2. Samenwerking tussen partijen is gestructureerd en erop gericht om met elkaar tot gepaste afspraken te komen voor de beoogde deling van persoonsgegevens. 3. De verwerkingsverantwoordelijke verkent de consequenties van internationaal delen van persoonsgegevens voor verwerkingen voor de organisatie. 4. De bewaking en administratie van de verdere verwerking, inclusief de vastgelegde en vastgestelde gronden vinden plaats op organisatieniveau. Van verwerken van persoonsgegevens in relatie

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

Onderbouwing score Betrokken partijen	
1 Afspraken maken en overeenkomsten sluiten met gebruik van modellen	
Onderbouwing kwaliteitsniveau:	Voor de meeste verwerkingen waarbij gegevens naar externe partijen worden verstuurd zijn verwerkersovereenkomsten of privacy-afspraken gemaakt voor zover nodig. Voor verwerkersovereenkomsten worden de ARBIT- of ARVODI-modellen van het Rijk gebruikt.
Ambitieniveau:	De Rechtspraak heeft nog niet voor alle externe datadelingen privacy-afspraken of een verwerkerssovereenkomst opgesteld. Wel heeft de Rechtspraak in beeld waarvoor nog overeenkomsten afgesloten moeten worden. Hier wordt aan gewerkt.
2 Documentatie onderlinge verhouding t.a.v. verwerking in keten- of andere samenwerking	
Onderbouwing kwaliteitsniveau:	Gezamenlijke verantwoordelijkheid komt vooral voor in de relatie tussen de Raad voor de rechtspraak en de gerechten. In deze relatie is de onderlinge verhouding vastgelegd in diverse governance documenten. Verder zijn er weinig gevallen waarbij sprake is van gezamenlijke verwerkingsverantwoordelijkheid. Bij datadeling tussen twee (niet gezamenlijke) verwerkingsverantwoordelijken worden afspraken gemaakt. Hiervoor zijn procedures opgesteld door het LDCR en IVO.
Ambitieniveau:	Op dit moment zijn er geen signalen die nopen tot acties om het kwaliteitsniveau te verhogen.
3 Doorgifte persoonsgegevens aan een derde land	
Onderbouwing kwaliteitsniveau:	In dit kader zijn 3 onderwerpen relevant: - Binnen de Rechtspraak zijn er 11 applicaties die persoonsgegevens buiten de Europese Economische Ruimte (EER) versturen. Hiervoor zijn verwerkersovereenkomsten opgesteld. Naar aanleiding van Schrems II wordt geïnventariseerd wat de gevolgen van de uitspraak voor de Rechtspraak zijn. - Gewerkt wordt aan digitale ondersteuning van het Gemeenschappelijk Hof van Justitie door diensten via het Rechtspraaknetwerk aan te brengen. - Cloudbeleid wordt opgesteld in afstemming met JenV.
Ambitieniveau:	Wanneer in kaart is gebracht wat de impact van de vernietiging van het Privacyshield is, kan hier actie op worden ondernomen. Daarnaast moet het cloudbeleid verder uitgewerkt worden, zodat duidelijke kaders volgen en richtlijnen uitgewerkt kunnen worden. Dit beleid wordt in samenwerking met JenV opgesteld en moet onder andere bevatten wie bevoegd is om risico's te accepteren.
4 Borgen informatiepositie en uitoefening rechten betrokkenen	
Onderbouwing kwaliteitsniveau:	Artikel 8 van de ARBIT- en ARVODI- template welke door de Rechtspraak wordt gebruikt, bepaalt dat de wederpartij zal ondersteunen bij de uitvoering van de rechten van betrokkenen. In dezelfde template wordt steeds opgenomen wie de wederzijdse contactpersonen zijn. Betrokkenen worden niet proactief geïnformeerd over de partijen waarmee de Rechtspraak overeenkomsten heeft afgesloten.
Ambitieniveau:	Op dit moment heeft de Rechtspraak nog geen signalen om het kwaliteitsniveau te verhogen.

Bijlage 1 Toelichting privacy management kpi's en kwaliteit

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

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

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

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

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

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

Bijlage 2. Invulformulier KPI aandachtsgebieden

Plaats voor alle zes de aandachtsgebieden van Privacy Administratie het betreffende cijfer (1 t/m 6) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Privacy Administratie**		
Organisatie score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	7. Er is centraal inzicht in (de status van) alle verwerkingen in het register van verwerkingen mogelijk door de FG, waarmee diens adviestaak (art. 35.2) wordt ondersteund. Bewaking op de naleving van maatregelen om tekortkomingen te mitigeren wordt (geautomatiseerd) gestructureerd ondersteund. 8. Er is centraal inzicht in (de status van, waaronder daarbij onder handen zijnde (herijkings)assessments in het kader van de Privacy Management Control Cyclus) voor alle DPIA's mogelijk voor de FG, waarmee diens adviestaak (art. 35.2) wordt ondersteund. 9. De organisatie beschikt over een toestemmingadministratie waaruit te allen tijde kan worden afgeleid wanneer en waarvoor toestemming is gegeven alsmede is ingetrokken. De relatie kan worden gelegd tot op de verwerkingsgerichte handeling waar de toestemming op van toepassing is. 10. Er is een workflow ingericht die de achtergronden van informatiebeveiligingsincidenten bij de bron (de melder) documenteert (en waar mogelijk direct mitigeert), de analyse hiervan (wel/geen (meldenswaardig) datalek) vormgeeft en de beschikbare tijd (max 72 klokuren) zo volledig mogelijk beschikbaar maakt voor de operationele afhandeling van datalekken. 11. Privacy beleid wordt periodiek en structureel binnen de Privacy Management Control Cyclus op de beoogde werking (instrueren van medewerkers omtrent de omgang met persoonsgegevens) herijkt en waar van toepassing aangepast en/of geactualiseerd. 12. Betrokkenen worden op gestructureerde wijze geïnformeerd omtrent het verwerken van hun persoonsgegevens vóórdat er sprake van verwerken is.
	4	Voorspelbaar	7. Het register van verwerkingsactiviteiten kent een nadere onderbouwing van elke verwerking. Op basis hiervan kan de kwaliteit van verwerkingen kan worden bewaakt en kan hierover op elk gewenst inhoudelijk niveau worden gerapporteerd. Het register van verwerkingsactiviteiten biedt hiermee tevens inzicht in de kwalitatieve ontwikkeling van verwerkingen in de tijd (periodieke herijkingen). Logging maakt onderdeel uit van de aandacht van de verwerkingsverantwoordelijke, om desgevraagd de handelingen die met persoonsgegevens zijn verricht tot op een diepgang die de AVG vereist (zie NEN 7513 als goed voorbeeld van een gedegen uitwerking hiervoor), te kunnen verantwoorden. 8. De risicoafweging van DPIA's worden gestructureerd en op eenduidige wijze gedocumenteerd. De naleving van het als actie benoemen, agenderen en door voeren van

			gesignaleerde verbeteringen, wordt bewaakt. De herhaalbaarheid van assessments is groot. Periodiek rapporteren aan management kan (geautomatiseerd) op eenvoudige wijze worden vormgegeven. 9. Er is een centrale registratie van toestemming en de status hiervan kan te allen tijde op verwerkingenniveau worden getoond. 10. Er is een duidelijk en binnen de organisatie geborgd protocol voor de afhandeling van datalekken. Uit de registratie van informatiebeveiligingsincidenten wordt periodiek lering getrokken. Verworven inzichten worden gebruikt in opleidingen voor medewerkers, bijvoorbeeld om dergelijke incidenten in de toekomst waar mogelijk te voorkomen (privacy bewustzijn vergroten) en bij de ontwikkeling van nieuwe (werk)processen, informatie-systemen, beleid en wetgeving. 11. Privacy beleid wordt actief uitgedragen binnen de organisatie, onder andere in opleidingen. 12. De publicatie van een privacyverklaring op internet is aangevuld met situationeel in te zetten informatiemateriaal. Dit materiaal dient om betrokkenen, zodra zij een raakvlak krijgen in een betreffende situatie, op correcte en gestructureerde wijze te informeren omtrent het verwerken van zijn/haar persoonsgegevens en de achtergronden daarvan.
	3	Vastgesteld	7. Het stramien van documenteren van verwerkingen in het register van verwerkingsactiviteiten vergroot de herhaalbaarheid (het herijken). Bovendien maakt het de daartoe vereiste effort (beslag op resources) acceptabel. Hierbij wordt doorontwikkeld aan het gestructureerd en geformaliseerd afhandelen van onderkende tekortkomingen en risico's voor de aandachtsgebieden van AVG art. 30 ergo het compliant werken en kunnen komen tot een verantwoorde maatregelenmix en bewaking van de naleving daarvan. 8. Het documenteren van DPIA's is omgeven met een workflow waarvan de beoordeling (kwaliteit/QA en juridisch) ervan een vast onderdeel uitmaakt. Het beoordelingsresultaat is opgenomen in de documentatie. 9. Verkrijgen en intrekken van toestemming bij verwerkingen wordt waar dit speelt eenduidig vastgelegd. Er wordt op toegezien dat al naar gelang op correcte wijze wordt gehandeld, zoals de verwerking waar toestemming voor nodig was maar die ingetrokken is, staken en daarbij vereiste handelingen verrichten (zoals bijvoorbeeld wissen). 10. Het centraal ondersteunen van incidentenregistratie, beoordeling, kwalificatie en afhandeling (waaronder datalekken) begint vorm te krijgen. 11. Er is een gestructureerd Privacy beleid dat door MT is vastgesteld. Dit beleid wordt actief uitgedragen naar personeel/medewerkers, onder meer via opleidingen. 12. Er is een privacyverklaring beschikbaar. Er wordt gewerkt aan procedures om de informatieplicht nader vorm te geven bij situationele verwerkingen.

	2	Beheerst	7. Er worden lokaal binnen de organisatie handmatig beheerde registraties van verwerkingen bijgehouden conform de AVG art.30 vereisten. De organisatie werkt aan een centrale registratie hiervoor. Bijkomend doel is lokale initiatieven voor dergelijke vastleggingen - waar van toepassing - te kunnen beëindigen. 8. Er wordt op gestructureerde wijze vormgegeven aan het opstellen en beheren van DPIA's op papier, uitgevoerd conform het Model Gegevensbeschermingseffect-beoordeling rijksdienst (PIA). 9. Gegeven toestemming wordt op procesniveau dus situationeel gedocumenteerd, evenals het eventueel weer intrekken hiervan. 10. Er is een situationele datalekkenprocedure. De beoordeling en afhandeling van informatiebeveiligingsincidenten worden ad hoc gevolgd. 11. Privacy beleid bestaat nog niet maar is inmiddels in ontwikkeling. 12. Een privacyverklaring is extern beschikbaar.
	1	Informeel	7. De verwerkingsverantwoordelijke verkeerd nog in de fase van ontdekken hoe efficiënt en effectief vorm te geven aan haar documentatieverplichtingen. De organisatie is hiertoe bezig zijn privacy verplichtingen uit te werken qua context en inhoud alsmede beheerbenadering. Er is op lokaal niveau lokaal een basale vastlegging van verwerkingen aan het ontstaan. 8. DPIA's c.q. risicoassessments worden ad hoc en situationeel op papier uitgevoerd conform het Model Gegevensbeschermingseffectbeoordeling rijksdienst (PIA). 9. Toestemming wordt impliciet aanwezig geacht indien persoonsgegevens worden verwerkt. Er vindt geen registratie van plaats. 10. Registratie en het volgen van informatiebeveiligingsincidenten alsmede de analyse of dit datalekken betreft wordt ad hoc en situationeel (waar het zich voordoet) geregeld. 11. Privacy beleid ontbreekt. 12. Er wordt gewerkt aan een centrale privacyverklaring voor de organisatie.

Plaats voor alle drie de aandachtsgebieden van Transparantie het betreffende cijfer (1 t/m 3) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Transparantie**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	4. Reacties van betrokkenen wordt gestructureerd meegenomen bij het opstellen, herijken, beheer en onderhoud van de communicatie en het informeren van betrokkenen over de verwerking van persoonsgegevens. 5. Betrokken worden altijd geïnformeerd over het verwerken van persoonsgegevens voordat dit plaatsvindt. 6. Betrokkenen kunnen informatie over verwerkingen eenvoudig vinden en worden geholpen om hun vragen daaromtrent te stellen.
	4	Voorspelbaar	4. Periodiek vindt binnen de Privacy Management Control Cyclus verificatie en toetsing plaats van de ingerichte werkwijze en procedures om betrokkenen passend te informeren omtrent (de achtergronden van) verwerkingen. 5. Het tijdig en adequaat informeren van betrokkenen omtrent verwerkingen maakt integraal onderdeel uit van de Privacy Management Control Cyclus. 6. Er is een (online) procedure ingericht voor betrokkenen bij verwerkingen om hun privacy rechten op eenvoudige wijze uit te kunnen oefenen.
	3	Vastgesteld	4. Het informeren van betrokkenen over verwerkingen en welke informatie daarbij wordt verwerkt is eenduidig, formeel en procesmatig vastgelegd. Er is consistentie in de uitvoering. 5. De organisatie beschikt over een privacyverklaring waarmee alle informatie omtrent verwerken door de organisatie namens de verwerkersverantwoordelijke voor betrokkenen op één plaats wordt aangeboden. Er kan eenvoudig nadere inhoudelijke informatie bij en over specifieke verwerkingen aan betrokkenen worden verstrekt. 6. Er zijn - waar proces technisch mogelijk - flyers of anderszins voorzieningen gecreëerd om betrokkenen vooraf te informeren omtrent het verwerken van persoonsgegevens op een zo begrijpelijk mogelijke manier (bijvoorbeeld in meer talen beschikbaar).
	2	Beheerst	4. Binnen de organisatie is vastgelegd wanneer en hoe betrokkenen vooraf worden geïnformeerd en welke informatie wordt verstrekt. 5. Er is duidelijk welke informatie verstrekt moet worden in het kader van de informatieplicht en er wordt gewerkt aan een manier om betrokkenen dit ook aan te reiken. 6. Er wordt gewerkt aan informatiemateriaal dat gebruikt kan worden om betrokkenen te informeren omtrent het verwerken van persoonsgegevens.
	1	Informeel	4. Er wordt gewerkt aan werkvormen voor het informeren van betrokkenen omtrent het verwerken van persoonsgegevens. 5. Of en hoe betrokkene wordt geïnformeerd en welke informatie wordt verstrekt is situationeel en sterk afhankelijk van keuze (en kennis op dit vlak) van de lijnverantwoordelijke binnen de organisatie.

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

Plaats voor alle drie de aandachtsgebieden van Privacy by Default het betreffende cijfer (1 t/m 3) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Privacy by Design/Default (PbD)**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	4. Voor nieuwe (of vernieuwde c.q. van een grote release voorziene) informatiesystemen, werkprocessen of wetgevingstrajecten is het principe van Privacy by Design en Default doorgevoerd in de maatregelenmix. Het bewaken van de implementatie van deze principes is geborgd binnen de Privacy Management Control Cyclus (op een voor de verwerkingsverantwoordelijke passend niveau) door registratie van de gedurende de ontwikkeling gemaakte privacy afwegingen in het register van verwerkingsactiviteiten. 5. Uit het register van verwerkingsactiviteiten zijn naast de verkozen maatregelenmix tevens de gemaakte afwegingen om tot een oplossingsrichting te komen af te leiden. 6. Voor verwerkingen waarbij keuzeafwegingen moeten worden gemaakt met een mogelijke impact op de persoonlijke levenssfeer van betrokkenen wordt bij het invullen altijd standaard de optie die de minste impact heeft op de betrokkene geselecteerd of er zijn organisatorische waarborgen ingesteld om dit te borgen.
	4	Voorspelbaar	4. Nieuwe verwerkingen worden alleen operationeel doorgevoerd (decharge) als aan alle privacy verplichtingen is voldaan gekenmerkt door aantoonbaarheid vanuit de Privacy Administratie. Dit omvat de maatregelenmix in het kader van Privacy by Design gedurende de ontwikkelfase periodiek geëvalueerd en getoetst is aan de stand der techniek (wat is er mogelijk) en uitvoeringskosten (wat kost dat) afgezet tegen de risico's die met de verwerking gepaard gaat en de aard van de te beschermen persoonsgegevens. 5. In de beschouwing van passende bescherming van persoonsgegevens bij verwerkingen wordt het belang van betrokkenen primair gesteld. Bij selectietrajecten om oplossingen te verwerven is het hier niet aan voldoen een showstopper voor de oplossingsvariant. 6. Er is gestructureerd aandacht voor het belang van bescherming van de persoonlijke levenssfeer van betrokkenen bij verwerkingen.
	3	Vastgesteld	4. Gedurende de gehele looptijd van een project/verwerking wordt periodiek de bescherming van persoonsgegevens gevalideerd voor de oplossingsrichting en daaruit ontleende oplossingsvariant. Deze activiteit wordt gedocumenteerd (aantoonbaar) in het register van verwerkingsactiviteiten op een zodanige wijze dat in het ontwerp van verwerkingen de bescherming van de persoonlijke levenssfeer van betrokkenen op een voor de verwerkingsverantwoordelijke passend niveau is verankerd. 5. De principes van Privacy by Design (vroegtijdig aandacht voor privacy) worden systematisch meegenomen als eis (must haves) in programma van eisen bij het verwerven van informatiesystemen.

			6. De bewaking van keuzeopties in informatiesystemen en processen in relatie tot de bescherming van de belangen van betrokkenen is in organisatorische procedures binnen de organisatie ingebed voor die verwerkingen waar het nog geen geautomatiseerde voorziening van de oplossing is.
	2	Beheerst	4. Aandacht voor privacy by design en default is standaard onderdeel van de projectenaanpak voor de ontwikkeling van processen, informatiesystemen, beleid of wetgeving. Op naleving van het rekening houden met deze privacy aandachts-punten in projecten wordt toegezien en gestuurd. 5. Bij het bepalen van de maatregelenmix rond verwerkingen wordt rekening gehouden met het belang van betrokkenen in het kader van de bescherming van de persoonlijke levenssfeer. 6. Er wordt nagedacht over het bepalen van keuzen met de minst grote impact en de manieren om te borgen dat die standaard als antwoord worden voorgelegd.
	1	Informeel	4. De aandacht voor privacy als aandachtsgebied wordt ad hoc en soms afhankelijk van de kennis hieromtrent binnen het project opgepakt bij het ontwerpen van processen, informatiesystemen of wetgeving. Het documenteren van de afwegingen rondom inrichting van de privacy aandachtsgebieden van verwerkingen is situationeel en nog niet gestructureerd ingericht. 5. De bepaling van de adequaatheid van de maatregelenmix is een open proces zonder duidelijke afwegingskaders. Dit is onderkend en hieraan wordt gewerkt 6. De keuzeopties in informatiesystemen hebben (komend uit de verpakking) een functionele, soms alfabetische of numerieke insteek, maar zijn daarmee niet per definitie een inrichting die passend is vanuit Privacy by Default oogmerk. Dit is onderkend en er wordt onderzocht hoe dat op te lossen.

Plaats voor alle vier de aandachtsgebieden van Betrokken partijen het betreffende cijfer (1 t/m 4) in de kolom 'Organisatie score' bij de proceskwaliteit die uw organisatie past			
Kritieke Prestatie Indicator	**Betrokken partijen**		
Organisatie Score	Niveau	Proceskwaliteit	Gerealiseerd
	5	Geoptimaliseerd	5. De afsprakenkaders voor het verwerken van persoonsgegevens zijn voor elke verwerking die hiervoor in aanmerking komt tussen de partijen afgestemd en op passende wijze aantoonbaar gedocumenteerd en actueel. 6. Bij delen van persoonsgegevens buiten de organisatiegrenzen worden de onderlinge verhoudingen (verwerkingsverantwoordelijke, verwerker, gezamenlijk verwerkingsverantwoordelijk) periodiek (binnen de Privacy Management Control Cyclus van 3 jaar) herijkt. 7. Er is een duidelijk kader en/of richtlijnen en vastgelegde structuur voor levering van persoonsgegevens met derde landen beschikbaar, die het vereiste beschermingsniveau van persoonsgegevens hierbij borgt. 8. Het hoger management stuurt op het volgens beleid correct verwerken van persoonsgegevens en monitort daarbij de naleving van de belangen van betrokkenen.
	4	Voorspelbaar	5. De afsprakenkaders tussen partijen zijn helder, effectief en efficiënt vastgelegd in daartoe geëigende en met elkaar vastgestelde formele documenten. 6. De onderlinge verhoudingen tussen de partijen is eenduidig met elkaar overeengekomen en gedocumenteerd. 7. Er is bij internationale doorgifte structureel aandacht voor het belang van de impact van adequaatheidsbeslissingen op de (on)rechtmatigheid van verwerkingen. Er vindt sturing plaats op de toepassing van het centraal bepaalde beleid m.b.t. vastlegging en vaststelling van de grond van de verder verwerking. 8. De wijze waarop invulling gegeven wordt aan de rechten van betrokkenen en het informeren over verwerkingen van betrokken is vastgelegd in processen.
	3	Vastgesteld	5. Er is duidelijk hoe verantwoordelijkheden liggen; eenzijdige verwerkingsverantwoordelijkheid, gezamenlijke verwerkingsverantwoordelijkheid, verwerker. 6. Samenwerking tussen partijen is gestructureerd en erop gericht om met elkaar tot gepaste afspraken te komen voor de beoogde deling van persoonsgegevens. 7. De verwerkingsverantwoordelijke verkent de consequenties van internationaal delen van persoonsgegevens voor verwerkingen voor de organisatie. 8. De bewaking en administratie van de verdere verwerking, inclusief de vastgelegde en vastgestelde gronden vinden plaats op organisatieniveau. Van verwerken van persoonsgegevens in relatie tot andere partijen is de rechtmatigheid vastgesteld en dit kan worden aantonen voor betrokkenen.

	2	Beheerst	5. Taken en verantwoordelijkheden van partijen bij verwerkingen worden structureel en gezamenlijk/in overleg geanalyseerd en beschreven. Bij het delen van persoonsgegevens tussen partijen wordt gewerkt met verwerkersafspraken (binnen de overheid) of verwerkersovereenkomsten (externe partijen). Vastleggen en stellen van doelen en beschermingsniveau geschiedt voor iedere verdere verwerking. 6. Reikwijdte en impact van kaders voor gegevensdelen zoals het adequaatheidsbeginsel of het memorandum van overeenstemming en de relatie hiervan met bijvoorbeeld de afdwingbaarheid van afspraken en onderbouwing van redenen van verwerken worden beschouwd. 7. Er vindt analyse plaats van verwerkingen binnen de organisatie waarin sprake is van doorgifte aan derde landen en/of internationale organisaties. 8. De bewaking van persoonsgegevens worden verwerkt volgens vastgelegde gronden en vindt plaats op afdelingsniveau.
	1	Informeel	5. De (werk)relatie tussen partijen is impliciet bepaald in het operationeel werkproces op basis van zich manifesterende situaties. 6. Taken en verantwoordelijkheden tussen partijen van verwerkingen zijn incidenteel beschreven. 7. Er is geen sprake van gegevenslevering aan landen buiten de EEG. 8. Er is georganiseerd dat betrokkenen namens verwerkingsverantwoordelijke worden geïnformeerd over verwerkingen van en door de organisatie, waarbij derden een raakvlak hebben in de verwerking.

Deelbesluit 10 - Datalekken
Document 342

Meldplicht datalekken

Alle bedrijven en overheden moeten datalekken direct melden aan de toezichthouder. Voor de Rechtspraak zijn dit de Procureur Generaal bij de Hoge Raad (bij datalekken in het kader van de gerechtelijke taak) en de Autoriteit Persoonsgegevens (voor overige datalekken). In sommige gevallen moeten datalekken ook gemeld worden aan de personen van wie de persoonsgegevens gelekt zijn.

Wat is een datalek?

We spreken van een datalek als derden die geen toegang zouden mogen hebben tot bepaalde persoonsgegevens, die informatie (mogelijk) toch in handen hebben gekregen. Ook de kans op een datalek geldt als datalek.

Bij een datalek kun je bijvoorbeeld denken aan een kwijtgeraakte usb-stick, een gestolen of verloren laptop of een zoekgeraakt dossier. Maar er is bijvoorbeeld ook sprake van een datalek als:

- dossiers door het raam van een geparkeerde auto te lezen zijn;
- geeltjes met persoonsgegevens aan monitors hangen en leesbaar zijn voor derden;
- kopietjes of printjes met persoonsgegevens in een afvalbak belanden in plaats van een beveiligde papiercontainer;
- het per abuis toevoegen van processtukken aan een onjuiste gemachtigde in één van de digitale webportalen.

Wanneer moet een datalek gemeld worden?

Een datalek moet gemeld worden aan de toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de personen van wie de gegevens zijn gelekt

Vanaf de ontdekking heeft een organisatie **72 uur de tijd** om een datalek bij de toezichthouder te melden. De ontdekking is het moment waarop we voor het eerst op de hoogte waren van een incident dat mogelijk onder de meldplicht datalekken valt. Melden wij het incident na deze termijn van 72 uur, dan moeten wij goed kunnen uitleggen waarom wij te laat waren. De toezicht kan boetes opleggen tot 10.000.000 euro als we niet aan onze meldplicht voldoen.

Mogelijk is 72 uur na de ontdekking van het incident nog niet volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval melden we het datalek op basis van de gegevens waarover we op dat moment beschikken.

Als een datalek - mogelijk - ongunstige gevolgen heeft voor de privacy van de betrokkenen, moet het datalek ook aan de betrokkenen worden gemeld. Dit gebeurt altijd in overleg met de afdeling communicatie van de organisatie waar het datalek heeft plaatsgevonden.

Welke organisatie moet een datalek melden?

Welke organisatie een datalek volgens de wet moet aanmelden bij wie, is weergegeven in onderstaande tabel:

Oorsprong datalek bij:	Melding aan toezichthouder door*:	Melding aan betrokkenen door*:
Gerecht	Gerecht	Gerecht
Landelijke dienst (IVO Rechtspraak, LDCR, SSR)	Betreffende landelijke dienst	Betreffende landelijke dienst
Raad voor de rechtspraak	Raad voor de rechtspraak	Raad voor de rechtspraak

* indien van toepassing

Hoe meld je als medewerker een datalek?

Heb je een mogelijk datalek veroorzaakt of heb je het zien gebeuren? Meld dit dan altijd direct aan twee functionarissen: je leidinggevende en de lokale beveiligingscoördinator.

Gaat het om verlies of diefstal van een digitaal apparaat (laptop, tablet of smartphone)? Neem dan allereerst zo snel mogelijk (24/7!) contact op met het KlantContactCentrum van IVO Rechtspraak:

- 07:30 - 20:00 uur: **088 - 361 7777**
- Na 20.00 uur (ook 's nachts): **088 - 361 3208**.

Op die manier kan het apparaat met spoed geblokkeerd en op afstand gewist worden (indien mogelijk).

Meld het vervolgens ook aan je leidinggevende en de lokale beveiligingscoördinator.

Twijfel je of sprake is van een (mogelijk) datalek? Overleg dan altijd met de beveiligingscoördinator van jouw gerecht of landelijke dienst.

Ben je zelf leidinggevende? Zorg dan dat je medewerkers weten dat ze elk (mogelijk) datalek direct aan jou melden.

Meer informatie?

Raadpleeg het *Handboek Meldplicht datalekken voor gerechten* (Intro) of neem contact op met je beveiligingscoördinator.

Deelbesluit 10 -Datalekken
Document 343

de Rechtspraak

Raad voor de rechtspraak

aan	Leden LOBRO
van	[redacted]
doorkiesnummer	06- 52 80 70 69
datum overleg	21 april 2022
aanwezig	[redacted] (vz.), [redacted]
afwezig	[redacted], Elmar Jonasse

LOBRO verslag

houdt geen verband met woo-verzoek

[redacted]

de Rechtspraak

Raad voor de rechtspraak

Uitkomsten datalek digitale postkamer
Zie mail van [redacted] van 20 april 2022 voor de uitkomsten.

Er zijn technische maatregelen genomen door IVO. Hiermee is het aantal adresseringsfouten aanzienlijk gereduceerd. Het gaat nu nog om fouten van (nieuwe) medewerkers die nog niet met systeem bekend zijn. [redacted] stelt voor om nieuwe datalekken automatische door te sturen naar de functionele datalekmailboxen van de gerechten. Het LOBRO stemt hiermee in. *Dit geldt alleen voor de rechtbanken.*

De memo en uitkomsten worden ter informatie doorgestuurd naar het SBO.

houdt geen verband met woo-verzoek

[redacted]

Deelbesluit 10 - Datalekken
Document 344

Privacybeleid
IVO-rechtspraak

Auteur:	SP&K
Versie:	1.0
Datum:	3 januari 2020
Vastgesteld op:	19 maart 2020

Inhoudsopgave

Versiebeheer

Versie	Wat	Door wie	Datum
0.1	Initieel	[redacted]	15-04-2019
0.2	Opmerkingen [redacted] en [redacted] verwerkt	[redacted]	01-05-2019
0.3	Opmerkingen [redacted] en [redacted] verwerkt	[redacted]	14-06-2019
0.6	Opmerkingen [redacted] verwerkt	[redacted]	17-07-2019
0.9	Voorgelegd aan [redacted], [redacted], [redacted], [redacted] en [redacted]. Opmerkingen [redacted], [redacted] en [redacted] verwerkt	[redacted] en [redacted]	01-08-2019
0.9	Voorgelegd aan directie ter vaststelling	[redacted]	03-01-2020
1.0	Vastgesteld door directie	[redacted]	19-03-2020

1 Visie op privacy

In dit hoofdstuk wordt op basis van wetgeving, regelgeving en intern beleid de visie op privacy binnen IVO-rechtspraak (hierna: 'IVO') beschreven. Deze visie gaat in op een aantoonbaar rechtmatige wijze van verwerking van persoonsgegevens. Dit sluit aan bij de uitgangspunten van de Algemene Verordening Gegevensbescherming (hierna: 'AVG')[1] en het privacybeleid dat binnen de Rechtspraak is gemaakt. Dit hoofdstuk bevat voorts de missie alsmede de uitgangspunten en randvoorwaarden om dit mogelijk te maken binnen IVO.

1.1 Wettelijk en beleidskader

Het recht op privacy binnen Nederland is vastgelegd in de Grondwet, meer specifiek art. 10 lid 2. Daarin staat dat iedereen recht heeft op eerbieding van zijn persoonlijke levenssfeer. Met de term persoonlijke levenssfeer wordt een gebied aangeduid waarbinnen elk individu vrij is en geen inmenging van anderen hoeft te accepteren. Beperkingen zijn alleen mogelijk wanneer deze in de wet geregeld zijn. Sinds 25 mei 2018 wordt het privacyregime hoofdzakelijk geregeld door de op Europees niveau vastgestelde AVG.

Artikel 24 AVG bevat de verplichting voor de verwerkersverantwoordelijke (in dit geval de Raad voor de rechtspraak en de gerechten gezamenlijk, maar in sommige gevallen ook IVO Rechtspraak als landelijke dienst van de Rechtspraak) om, rekening houdend met de aard, de omvang, de context, het doel van de verwerking en de privacyrisico's, passende technische en organisatorische maatregelen te nemen. De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerkingen in overeenstemming zijn met de AVG en de overige privacywetgeving. Tot slot moet de verwerkingsverantwoordelijke passend gegevensbeleid uitvoeren. Dit geheel moet (periodiek) geëvalueerd en indien nodig geactualiseerd worden.

De Raad voor de rechtspraak (hierna: 'de Raad') en de gerechten hebben hun beleidsverplichting vormgegeven in het Strategisch privacy plan[2] dat verder is uitgewerkt in het Privacybeleid Rechtspraak[3]. Voor IVO is het van belang om op basis van deze strategische normenkaders haar eigen beleid op te stellen, zodat ook zij kan aantonen:

- hoe de naleving van de beginselen en de grondslagen van de privacywetgeving ingevuld en aangetoond worden;
- hoe privacy binnen IVO wordt ingericht op basis van het strategisch privacybeleid van de Raad;
- dat binnen IVO duidelijk is wat van welke functionarissen verwacht mag worden om het risico van onrechtmatige verwerking van persoonsgegevens zo klein mogelijk te houden.

---

[1] VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

[2] [redacted]

[3] [redacted]

De rol van IVO als gegevensverwerker
In de privacywetgeving worden verschillende soorten rollen genoemd die gegevensverwerkers kunnen hebben. Op basis van deze rollen gelden rechten en plichten voor de organisatie die persoonsgegevens verwerkt. Vanwege de positie van IVO binnen en buiten de Rechtspraak is het van toegevoegde waarde om aan te geven welke rol IVO speelt in welke situaties. Om de rol te bepalen is gebruik gemaakt van de privacywetgeving, de Wet RO en het Instellings- en mandaatsbesluit IV-organisatie Rechtspraak.

- IVO is verwerkersverantwoordelijke wanneer het gaat om interne gegevens. Hier gaat het bijvoorbeeld om gegevens van medewerkers en bedrijfvoeringsinformatie
- IVO is verwerker wanneer het gaat om het verwerken van persoonsgegevens in niet-landelijke diensten en systemen.
- IVO is interne beheerder wanneer het gaat om persoonsgegevens in landelijke diensten en systemen.
- IVO is verwerker wanneer persoonsgegevens worden gewerkt van externe partijen, zoals de Commissies van Toezicht.

1.2 Visie en missie op privacy

IVO is de informatievoorzieningsorganisatie van de Rechtspraak. Dit betekent dat IVO er verantwoordelijk voor is dat de diensten die zij levert, voldoen aan wet- en regelgeving alsmede het beleid van de Raad en de gerechten als gezamenlijke verwerkersverantwoordelijke. Dit beleid is gebaseerd op wetgeving, regelgeving of intern beleid. Ook de visie op privacy van IVO is gebaseerd op de visie op privacy van de Rechtspraak.[4] Deze visie van de Rechtspraak maakt onderscheid in de categorie van de persoonsgegevens (normaal, gevoelig of bijzonder) en de soort gegevensverwerking (organisatorisch, ondersteunend of primair proces) om de mate van beveiliging te bepalen waarbij de wet als minimumnorm geldt.

In lijn met de visie van de Rechtspraak, gebaseerd op het Strategisch privacy plan, is het de visie van IVO om de diensten in lijn met bovenstaand principe in te richten. Dit betekent dat de gegevensverwerking van systemen in het primaire proces, zoals [redacted], zwaardere privacymaatregelen kennen dan systemen die het secundaire proces ondersteunen, zoals [redacted]. Ook hier wordt de minimum bepaald door de wet. Deze visie resulteert voor de primaire processystemen onder andere in zwaardere loggingseisen, hogere encryptie-eisen en een lagere acceptatiebereidheid van (privacy)risico's.

Uit eerdere rapportages die door IVO aan de Raad beschikbaar zijn gesteld, blijkt dat IVO wel in control, maar nog niet compliant, is. Dit betekent dat nog niet aan alle verplichtingen uit de AVG voldaan wordt, maar dat wel helder is wat moet gebeuren om aan alle verplichtingen te voldoen. Er is een planning die aangeeft welke stappen op welk moment genomen moeten worden om alle omissies weg te nemen. Het is dan ook de missie van IVO om de openstaande punten op basis van de planning op te lossen en compliant te worden met de verplichtingen uit de AVG. Hiervoor is een roadmap opgesteld.

---

4 [redacted]

1.3 Scope

Het beleidskader privacy is van toepassing op geheel IVO Rechtspraak. Binnen de scope vallen alle op dit moment geldende kaders op het gebied van privacy die door de wetgeving, de Raad van de Rechtspraak en door de IVO Rechtspraak directie opgelegd zijn.

Het privacybeleid is van toepassing op alle medewerkers, processen, diensten en producten.

1.4 Uitgangspunten en randvoorwaarden

Binnen het privacybeleid van IVO gelden de volgende uitgangspunten en randvoorwaarden:

- kennis van privacy is essentieel en moet geborgd worden;
- Wanneer zich situaties voordoen waarin het beleid en de wet niet in een heldere oplossing voorzien, dan is het hoogste aanwezige directielid van IVO bevoegd, na advies van de (plaatsvervangend) privacy officer, bevoegd de kwestie te beslechten. De Functionaris voor de gegevensbescherming van de Raad wordt van het besluit op de hoogte gebracht door de (plaatsvervangend) privacy officer.

1.5 Vervolg

In het vervolg worden beleidsregels geformuleerd voor de gehele levenscyclus van de diensten die IVO aan de Raad en de gerechten levert. Daarnaast wordt in dit document ook beleid opgesteld dat de verwerking van persoonsgegevens binnen IVO regelt als verwerkingsverantwoordelijke, verwerker en intern beheerder.

2 Taken, verantwoordelijkheden en bevoegdheden IVO

Omschrijving	Taken en verantwoordelijkheden
Raad voor de rechtspraak	Verantwoordelijk voor het opstellen en vaststellen van het overkoepelende Rechtspraak privacybeleid. Voorbeelden hiervan zijn de privacyvisie, normenkaders en bewaartermijnen.
CIO (Directeur IVO)	De CIO is eigenaar van het privacybeleid en daarmee eindverantwoordelijk voor dit beleid en de inrichting ervan in de staande organisatie. Controle en toezicht op naleving van dit beleid is gedelegeerd aan de teamleider Security, Privacy & Kwaliteit (SP&K). De CIO is eindverantwoordelijk inzake alle privacy gerelateerde onderwerpen binnen IVO voor zover de eindverantwoordelijkheid niet bij de Raad ligt.
Directie van IVO	De directie van IVO is verantwoordelijk voor: • Vaststellen van het privacybeleid • Het implementeren, uitvoeren en handhaven van het privacybeleid • Het beschikbaar stellen van voldoende middelen voor de uitvoering van het privacybeleid. • Het aanstellen van een privacy officer en teamleider SP&K. • Het vaststellen van de visie en strategie op privacy voor IVO.
(plaatsvervangend) Privacy Officer (PO)	De privacy officer is verantwoordelijk voor: • Het opstellen en jaarlijks evalueren van het privacybeleid. • Het onder verantwoordelijkheid van de Raad bijhouden van het landelijke register verwerkingen. • Het melden van mogelijke datalekken binnen IVO bij het datalekteam, de Autoriteit Persoonsgegevens en/of de Procureur Generaal bij de Hoge Raad. • Controle op en toetsing van het interne privacybeleid en de naleving daarvan. • Controle op juiste uitvoering van PIA • De privacycultuur en -bewustwording. De privacy officer heeft bij het uitvoeren van de interne controle op privacy de bevoegdheid om informatie op te vragen bij de directie, teamleiders, managers en portefeuillehouders.
Functionaris voor de gegevensbescherming (FG)	De FG geeft advies in het kader van privacyaangelegen binnen IVO. Zo beoordeelt de FG de PIA's die zijn opgesteld en geeft de FG daarover een advies af.
Contractmanager	De contractmanager is verantwoordelijk voor: • Het overzicht van verwerkersovereenkomsten en verwerkersafspraken.

	• Het ondersteunen bij het opstellen van verwerkersovereenkomsten
Teamleider SP&K	De teamleider SP&K is gedelegeerd verantwoordelijk voor: • Uitzetten van acties (na risicoafweging) indien het privacybeleid niet wordt nageleefd; • Het nemen van operationele beslissingen (na risicoafweging) aangaande privacy waarin dit beleid (nog) niet voorziet; • Richting geven aan het borgen van de privacy binnen IVO Rechtspraak. De teamleider SP&K is, indien zwaarwegende redenen hiertoe nopen, bevoegd om direct contact op te nemen met de portefeuillehouder privacy en de FG bij de Raad. De directeur IT van IVO wordt hiervan door de teamleider SP&K op de hoogte gesteld.
Portefeuillehouders	De portefeuillehouders zijn verantwoordelijk voor: • de bestaande en nieuwe informatievoorziening binnen hun portefeuille. Deze moet voldoen aan de privacywetgeving en het privacybeleid • zorgdragen voor voldoende middelen om ervoor te zorgen dat de informatievoorziening binnen portefeuille voldoen aan de privacywetgeving
Dienstenmanager	De dienstenmanagers zijn er verantwoordelijk voor: • dat de diensten binnen zijn/haar portefeuille gaan voldoen en vervolgens te allen tijde blijven voldoen aan privacywetgeving. Hiervoor kan onder andere gebruik worden gemaakt van de opsomming in paragraaf 3.6 • dat er voldoende capaciteit is om compliancy te waarborgen • het rapporteren aan de privacy officer over de onderde eerste bullet genoemde punten en eventuele afwijkingen op de privacywetgeving.
Leidinggevenden	Alle leidinggevenden zijn verantwoordelijk voor: • het uitvoeren en uitdragen van het privacybeleid • het vastleggen van verwerkingen binnen de afdeling en het informeren daarover van de privacy officer • het inschakelen van de contractmanager voor het sluiten van een verwerkersovereenkomst waar nodig. • het signaleren van en rapporteren over privacymisstanden en –incidenten aan de privacy officer
Medewerkers SP&K	De medewerkers SP&K hebben de volgende verantwoordelijkheden: • maatregelen (laten) treffen in het geval van privacybedreigingen en -incidenten. • initiëren en adviseren betreffende maatregelen aangaande het privacybewustzijn van IVO medewerkers

	• het geven van advies en ondersteuning met betrekking tot normenkaders, beleid, principes en standaarden inzake privacy
Medewerker IVO Rechtspraak	Alle medewerkers van IVO zijn verantwoordelijk voor: • het uitdragen en naleven van het privacybeleid • het inschakelen van de leidinggevenden en/of privacy officer bij kwesties met betrekking tot privacy. • het melden van privacyincidenten bij het KCC van IVO

3 Privacy in de levenscyclus van diensten

Privacy is van belang gedurende de levenscyclus van informatiesystemen en diensten. In dit hoofdstuk wordt op basis van de secure software development lifecycle ingegaan op regels die gehanteerd worden moeten bij iedere fase van de levenscyclus. Hierbij is aandacht voor het aanschaffen, ontwikkelen en hergebruiken van (stukjes) dienstverlening.

Hieronder wordt aangegeven hoe in iedere stap van de levenscyclus van de informatievoorziening binnen IVO wordt omgegaan met privacy. Hierbij worden ook securityonderdelen genoemd worden, omdat security randvoorwaardelijk is voor privacy. Bij de concretisering wordt verwezen naar de respectievelijke securitykaders. Per bullet wordt aangegeven in welk hoofdstuk de onderdelen geconcretiseerd worden.

- Training en vergroten van privacy bewustzijn bij ontwikkelaars en beheerders (paragraaf 3.1)
- Requirementsfase (paragraaf 3.2):
    - uitvoeren van een risicoanalyse en een (data) privacy impact analyse;
    - formuleren security- en privacyrequirements;
    - bepalen quality gates
- Hergebruik, kopen of bouwen (paragraaf 3.3):
    - Threat modeling per epic/ use case
- Realisatiefase en testfase (paragraaf 3.4):
    - Gebruik standaardcode
    - Code review
    - Automatische (beveiligings)testen
    - Penetratietest
- Implementatiefase (paragraaf 3.5):
    - Security review
    - Akkoordverklaring systeem
- Operationele fase (paragraaf 3.6):
    - Patchmanagement
    - Uitfaseren van data en systemen

3.1 Training en vergroten van privacy bewustzijn

Training en vergroten van privacy bewustzijn is van essentieel belang om een datalek te voorkomen. Een datalek wordt gedefinieerd als: *"een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens"* (art. 4 lid 12 AVG).

Opleiding van ontwikkelaars en beheerders voor privacy heeft twee raakgebieden:

a. Security: een datalek kan ontstaan door een incident dat de beveiligingsmaatregelen van systemen bewust of onbewust omzeilt. Voorbeelden hiervan zijn een hackaanval of virusinfectie.
b. Privacy: een datalek kan ontstaan doordat een gebruiker een actie uitvoert en hierdoor bewust of onbewust persoonsgegevens lekt. In dit geval is er geen sprake van het bewust of onbewust omzeilen van beveiligingsmaatregelen, zoals het verkeerd adresseren van een e-mail of het verliezen een laptop.

De opleiding van ontwikkelaars en beheerders op het gebied van punt a. valt niet onder dit beleidsdocument. Hiervoor wordt bewezen naar het securitybeleid[5].

Voor de opleiding van ontwikkelaars en beheerders gelden de volgende regels:

a. De medewerkers krijgen jaarlijks een training die gericht is op privacy die past bij hun werkzaamheden. De managers en meewerkend teamleiders faciliteren hun medewerkers hierin.
b. Er wordt aangesloten bij het bewustmakingsprogramma van de Raad voor de rechtspraak waarin ook het belang van privacy in aan bod komt.

3.2 Requirementsfase

Een requirement in de IT is een eis of wens aangaande een IT-systeem. Hierin kan een onderscheid gemaakt worden in functionele en niet-functionele requirements. Een functionele geeft het gewenste gedrag weer van een systeem. Het betreft de behoefte van de business die een bepaalde actie met een IT-systeem wil uitvoeren. Een niet-functionele requirement is een kwaliteitseis waaraan het systeem moet voldoen.[6] Gedurende de requirementsfase wordt in kaart gebracht aan welke eisen en wensen een nieuw IT-systeem moet voldoen.

Een deel van de niet-functionele privacy requirements wordt bepaald op basis van de privacy impact assessment (PIA). De resultaten hiervan worden op de backlog van het project of wijziging geplaatst. Het beleid inzake de PIA wordt verder uitgewerkt in paragraaf 3.3.1.

Op basis van de resultaten van de PIA worden quality gates bepaald. Het project moet ervoor zorgen dat aan alle quality gates voldaan is, voordat de stuurgroep decharge verleent aan het project.

De verantwoordelijkheid voor het ophalen van de privacyrequirements en het uitvoeren van de PIA ligt bij de opdrachtgever van het project.

---

[5] Zie informatiebeveiligingsbeleid IVO Rechtspraak.docx
[6] de Swart, 2010

3.2.1 Privacy impact assessment

Een PIA is een hulpmiddel om bij ontwikkeling van IV-systemen privacyrisico's op gestructureerde en heldere wijze in kaart te brengen. De PIA is geen vrijblijvende vragenlijst. Het is een vragenlijst die zowel richtinggevend als corrigerend bedoeld is. Daarnaast moet het beantwoordingsproces ook bewustwording stimuleren voor uiteenlopende privacyaspecten, zodat daar rekening mee wordt gehouden bij het ontwikkelen van systemen.

Wanneer

Het beleidsuitgangspunt is dat een PIA een vast onderdeel in een project of een wijziging in de verwerking van de persoonsgegevens van bestaande systemen. Met laatstgenoemde wordt bedoeld: een wijziging in

- de persoonsgegevens die worden verwerkt; of
- de technische en organisatorische maatregelen die zijn genomen om de verwerking van persoonsgegevens te beschermen.

Proces en rapportage

De PIA's worden uitgevoerd conform de hiervoor opgestelde procedure[7] op het meest recente format van het Rijk zoals dat is aangepast voor de Rechtspraak en opgeslagen op de privacysite op Intro.

3.3 Hergebruik, kopen of bouwen

Als de requirements voor een nieuwe dienst duidelijk zijn, wordt op basis van het principe 're-use, before buy, before build' een afweging gemaakt of deze behoefte ingevuld kan worden door het hergebruik van reeds aanwezige producten, het aanschaffen van nieuwe producten of door zelf te programmeren.

3.3.1 Hergebruik van producten, systemen of diensten

Bij hergebruik van producten, systemen of diensten worden (onderdelen) van al aanwezige producten, systemen of diensten gebruikt om een andere behoefte in te vullen. Wanneer (deels) voor hergebruik gekozen wordt, moet rekening gehoudenworden met de privacyeisen en de eisen uit het product, systeem of dienst die (deels) hergebruikt worden. Zo kunnen in het nieuwe systeem andere persoonsgegevens verwerkt worden waarvoor strengereeisen gelden. Hiervoor moet een gap-analyse uitgevoerd worden.

Verder moet bij het hergebruik rekening gehouden worden met het beveiligingsniveau. Door het kopiëren van software kunnen kwetsbaarheden ook gekopieerd worden wanneer deze al aanwezig waren of (opnieuw) geïntroduceerd worden wanneer het nieuwe product, systeem of dienst onvoldoende mitigerende maatregelen kent. Het is aan de dienstenmanager om hier rekening mee te houden.

3.3.2 Kopen van producten, systemen of diensten

Bij het kopen van nieuwe producten, systemen of diensten moet rekening gehouden worden met de privacyrequirements die gedurende de requirementsfase zijn opgesteld. Deze privacyrequirements worden meegenomen bij de uitvraag/request for proposal en worden gescoord door een medewerker van SP&K.

[redacted]

3.3.3 Bouwen van producten, systemen of diensten

Voorafgaand aan de bouw van functionaliteit moet duidelijk zijn wat gebouwd moet worden en hoe dit gebouwd moet worden. Concreet betekent dit het volgende voor het privacybeleid:

a. Voorafgaand aan de realisatie van een functionele behoefte is duidelijk of en wat er aan privacymaatregelen genomen moet worden. Hiervoor wordt aangesloten bij secure by design en threat modeling. De resultaten worden per use case toegevoegd in het betreffende systeem (bv. Jira).
b. De niet-functionele privacyaspecten die behorende tot een use case, zoals logging, kunnen niet losgemaakt worden van een use case.
c. De PIA en het verwerkingsregister worden bijgewerkt op basis van de privacymaatregelen die als gevolg van een use case (extra) genomen worden.
d. Gedurende projecten kunnen zich wijzigingen in de scope of functionaliteit voordoen. Deze wijzigingen worden vergelijkbaar met punt a. en punt c. uitgewerkt.

3.4 Realisatie- en testfase

In de realisatiefase worden de requirements uitgewerkt door middel van de stories die de functionaliteit en kwaliteitseisen beschrijven. Hiervoor wordt aangesloten bij security by design, privacy by design en privacy by default. Dit betekent dat gedurende de ontwikkeling gebruik wordt gemaakt van standaardcode, dat code review plaatsvindt, en de kwaliteitseisen voor privacy (automatisch) per use case getest worden. Standaardinstellingen worden op de minst gegevensverwerkende mogelijkheid geplaatst. Gebruikers kunnen deze instellingen naar gelieve aanpassen om meer persoonsgegevens te (laten) verwerken. Verder wordt software dusdanig gebruikt, zodat de code op een later moment opnieuw te gebruiken is. Goede documentatie is dus van belang.

Gedurende de testfase worden ook de maatregelen die het resultaat zijn van de PIA uitgewerkt. Dit kunnen zowel technische maatregelen, die in het systeem verwerkt worden, als procedurele maatregelen zijn. Voor het testen van use cases wordt geen gebruik gemaakt van productiedata. Onder voorwaarden kan gebruik gemaakt worden van geanonimiseerde productiedata. Dit staat verder uitgewerkt in het Beleid gebruik productiedata voor testdoeleinden.

Voordat nieuwe functionaliteit aan de gebruikers in productie ter beschikking wordt gesteld, wordt in de testfase een pentest gedaan conform het securitybeleid dat hierover gaat. Hierdoor is vanuit privacyperspectief zekerheid over de opzet, bestaan en werking van de geïmplementeerde beveiligingsmaatregelen. Wanneer het niet mogelijk is om een pentest uit te voeren, moet op een andere manier aangetoond worden dat de software veilig is voor de (persoons)gegevens die verwerkt worden.

3.5 Implementatiefase

Voorafgaand aan de implementatie van het gerealiseerde systeem wordt onder andere aan de hand van het overzicht in MISS gecontroleerd of aan alle eisen is voldaan. Dit betekent dat aan de volgende beleidsregels is voldaan:

- er is goedkeuring vanuit de functionaris gegevensbescherming op de PIA;
- de wijze waarop de requirements zijn ingevuld, is goedgekeurd door de privacy officer van IVO.
- de bevindingen uit de PIA zijn opgelost, overgedragen aan beheer/support of het geassocieerde risico is geaccepteerd;
- het systeem is opgenomen in het verwerkingenregister;

- waar nodig zijn verwerkersovereenkomsten gesloten of verwerkersafspraken gemaakt; en
- vanuit SP&K is positief geadviseerd op het gebied van informatiebeveiliging.

Om te bepalen wie bevoegd is om een (resterend) privacyrisico te accepteren, kan gebruik worden gemaakt van onderstaande tabel.

Score	Classificatie	Acceptatie bevoegde
1 t/m 2	Geen	Portefeuillehouder
3 t/m 4	Laag	Portefeuillehouder na advies (plv.) privacy officer
5 t/m 10	Midden	Portefeuillehouder na advies (plv.) privacy officer en overleg FG
12 t/m 15	Hoog	Directeur K&K na advies (plv.) privacy officer en FG
16 t/m 25	Urgent	IVO directie na advies (plv) privacy officer en FG

3.6 Operationele fase

Na een project of wijziging wordt een systeem (weer) in beheer genomen. De dienstenmanager is ervoor verantwoordelijk dat de diensten die hij in beheer heeft, gaan voldoen en blijven voldoen aan de geldende privacy- en beveiligingseisen.

In de gevallen beschreven in paragraaf 3.3.1 wordt wederom een PIA uitgevoerd of wordt de bestaande PIA aangepast om ervoor te zorgen dat het systeem compliant blijft. De dienstenmanager van de beheerafdeling zorgt ervoor dat er voldoende capaciteit is om compliancy te waarborgen en rapporteert hierover richting de privacy officer. De portefeuillehouder zorgt voor voldoende (financiële) middelen. De dienstenmanager is er verantwoordelijk voor dat de dienst te allen tijde blijft voldoen aan de opsomming in paragraaf 3.6

In de operationele fase gelden de volgende privacyregels:

- Bij het uitfaseren van een systeem wordt alle informatie die bewaard hoeven worden, verwijderd. Hiervan wordt melding gemaakt bij de privacy officer.
- Er is up-to-date beeld van het IV-landschap van IVO Rechtspraak.
- Alleen in de productieomgeving zijn persoonsgegevens aanwezig, tenzij goedkeuring is gegeven conform het beleid ‘Gebruik productie voor testdoeleinden’.
- Technisch beheerders en applicatiebeheerders hebben geen toegang tot productiedata, inclusief bestandsnamen, tenzij:
    - Dit noodzakelijk is om een probleem op te lossen;
    - De gebruiker goedkeuring heeft gegeven of heeft de informatie zelf verstrekt in het kader van een probleem. De verstrekte informatie moet deels verwijderd worden indien deze van gevoelige of vertrouwde aard is, zoals het BSN of informatie over een minderjarige.
    - Er een schriftelijke opdracht is van een bevoegde instantie, bijvoorbeeld in het kader van een integriteitsonderzoek.

4 Verwerkersovereenkomsten en verwerkersafspraken

Een verwerker is een persoon of organisatie die persoonsgegevens namens de Rechtspraak verwerkt. Dit betekent dat de andere persoon of organisatie de gegevens op eigen gezag verwerkt, maar wel binnen de kaders en doelen die door de Rechtspraak zijn bepaald.

De verwerking door een verwerker wordt geregeld in een overeenkomst, de zogenoemde verwerkersovereenkomst (art. 28 lid 3 AVG). In deze overeenkomst is vastgelegd dat de verwerker afdoende garanties heeft om de persoonsgegevens te beschermen.

Indien een verwerker onderdeel is van de Staat der Nederlanden, bijvoorbeeld: CJIB, DJI, DI&I of het Ministerie van Economische Zaken, dan hoeft geen verwerkersovereenkomst afgesloten te worden, maar moeten verwerkafspraken gemaakt worden.

Voorafgaand aan het testen met (persoons)gegevens uit de productieomgeving wordt een verwerkersovereenkomst of verwerkersafspraak met de verwerkende partij getekend. De ondertekening van deze documenten vindt plaats door het tekenbevoegde lid van de directie van IVO.

De procedure voor het opstellen van verwerkersovereenkomsten en –afspraken staat in de bijbehorende beschrijving[8]. Zoals uit hoofdstuk 2 is gebleken is de dienstenmanager ervoor verantwoordelijk dat de verwerkersovereenkomst tijdig opgesteld en onderhouden wordt.

5 Verwerkingenregister

De gerechten, de landelijke diensten en de Raad zijn verplicht om een register bij te houden van de verwerkingen die plaatsvinden binnen de Rechtspraak. De verwerkingen die landelijk plaatsvinden worden opgenomen in het landelijke verwerkingsregister van de Raad. IVO is onder verantwoordelijkheid van de Raad belast met het opstellen en bewerken van het landelijk verwerkingenregister. Deze bevoegdheid is gemandateerd naar de privacy officer van IVO Rechtspraak. De portefeuillehouders stellen per dienst in hun portefeuille de doelen en middelen vast.

De procedure voor verwerkersovereenkomsten en –afspraken staan in de bijbehorende beschrijving[9].

6 Datalekken binnen IVO

Van een datalek is sprake wanneer: “Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens” (art. 4 lid 12 AVG). Hier is sprake van wanneer iemand kennis neemt van informatie waartoe die persoon niet bevoegdheid is, bijvoorbeeld meelezen in de trein of verliezen van een versleutelde gegevensdrager.

Indien een datalek plaatsvindt binnen IVO, wordt de privacy officer door middel van het daarvoor opgestelde formulier[10] geïnformeerd. Vervolgens wordt een risicobeoordeling uitgevoerd gebaseerd op

de door ENISA opgestelde methodologie[11] ter beoordeling van de ernst van inbreuken op persoonsgegevens, aan de hand waarvan een inschatting gemaakt kan worden van de ernst en impact voor de betrokkene(n) en of het datalek mogelijk moet worden gemeld aan de toezichthoudende instantie en in sommige gevallen direct aan de betrokkene(n). Dit is een door de AP en WP29 (nu EDPB) geaccepteerde methodologie.[12] De officer meldt bij de FG van de Raad voor de rechtspraak die melding doet bij de toezichthoudende privacy instantie.

7 Controle bevoegdheid

De (plaatsvervangend) privacy officer voert in het kader van de interne controle periodiek compliancy assessments op diensten uit. De resultaten hiervan worden opgeslagen op de openbare privacysite en gedeeld met SDM'er, dienstenmanager, de directie van IVO, de FG van de Raad en de directeur Bureau Raad. De privacy officer heeft bij het uitvoeren van de interne controle op privacy de bevoegdheid om informatie op te vragen bij de directie, teamleiders, managers en portefeuillehouders. Zij zijn verplicht om die informatie binnen redelijke termijn, gesteld door de (plaatsvervangende) privacy officer, te leveren. Bij verschil van inzicht kan het informatieverzoek voorgelegd worden aan de directeur IT die een beslissing neemt. Bij niet of te late levering is heeft de priacy officer de mogelijkheid om te escaleren naar de directie van IVO.

Indien blijkt dat niet wordt voldaan het interne privacybeleid en de privacywetgeving, dan wordt een plan van aanpak, inclusief planning, opgesteld om daar weer aan te voldoen.

8 Logging

Goede logging is noodzakelijk voor verschillende onderdelen van de verschillende privacywetgeving. Zo is logging noodzakelijk om correcties door te voeren en beveiligingsmaatregelen te evalueren. Voor logging die in lijn is met de privacywetgeving wordt aangesloten bij D-I.3b.04 IT-normenkader Logging[13].

9 Privacy op de werkvloer

Dagelijks worden door IVO persoonsgegevens verwerkt in het kader van de arbeidsrelatie of de veiligheid binnen en rondom het pand. In dit hoofdstuk wordt beschreven hoe IVO met deze verwerkingen omgaat.

[redacted]

9.1 Cameratoezicht

Het cameratoezicht binnen IVO is gebaseerd op de normen uit de Minimumnorm Cameratoezicht. Verwerking van gegevens via het camerasysteem van IVO mogen alleen gebruikt worden wanneer ze gerelateerd kunnen worden aan de doelen omschreven in paragraaf 2.1 van vorengenoemde minimumnorm.

9.2 Integriteitsonderzoeken

Integriteitsonderzoeken worden binnen IVO uitgevoerd conform het Protocol Onderzoek Integriteitsschendingen.

9.3 Privacybewustzijn

Voor het bevorderen van het privacybewustzijn van de medewerkers van IVO gedurende alle fase van het dienstverband, wordt aangesloten bij de Minimumnorm veiligheids- en beveiligingsbewustzijn en die hieruit voortvloeiende bewustwordingsacties.

10 Clouddiensten

Voor de vereisten bij het gebruik van alle vormen van clouddiensten wordt aangesloten bij het Normenkader Clouddiensten. [14]

14 [redacted]

Deelbesluit 10 - Datalekken
Document 345

de Rechtspraak

aan	Raad voor de rechtspraak
van	[redacted]
datum	30 maart 2022
bijlage(n)	1
onderwerp	Achtste borgingsplan Rechtspraak

Toelichtende notitie achtste borgingsplan:

Stand van zaken ten aanzien van privacy binnen de Rechtspraak tot 1 februari 2022

Inleiding

In het Strategisch Plan Privacy is als algemeen uitgangspunt geformuleerd dat er te allen tijde in overeenstemming met de privacywet- en regelgeving wordt gehandeld. Dit waarborgt een zorgvuldige gegevensverwerking. Hierbij moet steeds een afweging gemaakt worden tussen het belang van privacy en andere belangen, zoals de openbaarheid van de Rechtspraak.

De Rechtspraak is echter nog niet zo ver dat te allen tijde in overeenstemming met de privacywet- en regelgeving wordt gehandeld. Het borgingsplan maakt inzichtelijk waar de Rechtspraak ten aanzien van dit uitgangspunt staat, waar de Rechtspraak naartoe wil en welke activiteiten ondernomen moeten worden om het gat hiertussen te overbruggen. Deze activiteiten beogen niet alleen te voldoen aan de verplichtingen van de Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG (UAVG), maar ook aan de verplichtingen die voortvloeien uit de Wet justitiële en strafvorderlijke gegevens (Wjsg) en bijbehorende regelgeving.

Het borgingsplan is voor het eerst opgesteld ter afronding van het Project AVG van het Bureau Raad op 25 mei 2018. Inmiddels ligt de achtste versie van het document voor.

Scope van het borgingsplan

Het borgingsplan is primair gericht op gegevensverwerkingen door de Raad en IVO Rechtspraak, omdat de meeste privacymaatregelen daar moeten worden genomen. Desalniettemin hebben de gerechtsbesturen ook de verantwoordelijkheid om privacy op lokaal niveau te waarborgen en hierover te rapporteren. Waar mogelijk geeft het borgingsplan een beeld over de mate waarin de gerechten de privacywet- en regelgeving hebben geïmplementeerd. Hiervoor wordt gebruik gemaakt van de uitvragen die plaatsvinden via het Key Control Dashboard en gesprekken met beveiligings- en privacycoördinatoren.

Doel

Het achtste borgingsplan betreft de stand van zaken tot 1 februari 2022. Met dit borgingsplan wordt de Raad geïnformeerd over de stand van zaken betreffende de implementatie van de AVG, UAVG en Wjsg (paragrafen 1 en 2).

Daarnaast wordt de Raad verzocht in te stemmen met de voorgestelde kwaliteits- en ambitieniveaus. De hiervoor benodigde acties zijn reeds geïnventariseerd en belegd (paragraaf 3).

1. Beeld Rechtspraak

Tot het zesde borgingsplan (1 februari 2021) werd in het borgingsplan gerapporteerd dat de Rechtspraak in control was. Sinds het zesde borgingsplan – en ook nu - wordt geconcludeerd dat de Rechtspraak niet volledig in control of compliant is met de geldende privacywet- en regelgeving.

Met in control wordt bedoeld dat nog niet op alle onderdelen aan de geldende privacywet- en regelgeving wordt voldaan, maar dat wel duidelijk is wanneer hieraan zal worden voldaan. Met compliant wordt bedoeld dat alle aan onderdelen van de privacywet- en regelgeving wordt voldaan en dat de onderdelen zijn geborgd. Hierbij moet de kanttekening gemaakt worden dat nooit sprake kan zijn van 100% compliancy.

2. Ontwikkelingen sinds 1 februari 2022

De peildatum van het achtste borgingsplan is 1 februari. Sindsdien hebben de ontwikkelingen niet stilgestaan. Vier ontwikkelingen worden hieronder uitgelicht:

1. Verbeteringen van de informatievoorziening in het kader van de privacywet- en regelgeving

Sinds het zesde borgingsplan heeft de Raad meermaals met de directie van IVO Rechtspraak gesproken over de verbeteringen in het IT-landschap, de bijbehorende planning en de eventuele acceptatie van risico's. Een overleg over dit onderwerp heeft voor het laatst plaatsgevonden tijdens de Raadsvergadering van 16 februari 2022. Door de directie van IVO Rechtspraak is een notitie ingebracht inzake de huidige stand van zaken van de AVG en Wjsg bij IVO Rechtspraak.

Tijdens de vergadering is geconstateerd dat de notitie geen planning bevatte. Dat is voor de Raad onvoldoende. De Raad wil inzicht krijgen in de planning en de risico's die de Rechtspraak loopt door bepaalde systemen niet of later te verbeteren. Op basis van de huidige versie kunnen zij niet bepalen hoe de Rechtspraak ervoor staat. Alle leden van de Raad willen op de hoogte zijn. Naar verwachting presenteert IVO Rechtspraak op korte termijn de planning en het overzicht Afhankelijk van de uitkomst wordt de conclusie ten aanzien van in control c.q. compliancy in het borgingsplan bij herijking in juli 2022 aangepast.

2. Beleidslijn bewaartermijnen van persoonsgegevens ten behoeve van niet-zaaksgebonden processen en systemen

Verder is in opdracht van het Bureau BVA een onderzoek uitgevoerd naar de bewaartermijnen van persoonsgegevens in niet-zaaksgebonden processen en systemen. De resultaten van dit onderzoek moeten leiden tot een eerste beleidslijn die aansluit op de beleidslijn bewaren van persoonsgegevens in primaire processystemen. Dit laatste document is besproken in de SBO-vergadering van 14 februari 2022.

3. Herziening Wjsg/Wpg

Begin maart 2022 is het Bureau Raad geïnformeerd over de beëindiging van de herziening van de Wet justitiële en strafvorderlijke gegevens en de Wet politiegegevens. De verantwoordelijke minister heeft hiervoor gekozen, omdat het regeerakkoord niet voorziet in de benodigde financiering van het project. Mocht op een later moment toch een probleem geconstateerd worden, dan wordt binnen de financiële kaders naar een oplossing gezocht.

4. Verbeteringen naar aanleiding van adresseringsfouten via de digitale postkamer

Begin februari 2022 zijn rechtbanken geïnformeerd dat in de periode 10 februari 2020 tot 25 januari 2022 3153 zijn geweest die kunnen worden aangeduid als datalek. Deze datalekken werden veroorzaakt door foutieve adressering via de digitale postkamer. Sindsdien is nader onderzoek gedaan en zijn technische en organisatorische maatregelen doorgevoerd. Hierdoor vinden de datalekken slechts sporadisch plaats. In de gevallen dat datalekken plaatsvinden, gaat het om een fout van een nieuwe medewerker.

Gezien de overwegingen van de product owner digitale postkamer en het kleine aantal meldingen sinds de reeds geïmplementeerde maatregelen, lijken aanvullende technische maatregelen op dit moment niet noodzakelijk. Bij de rechtbanken wordt nogmaals aangegeven hoe belangrijk melden in Classbase is, zodat eerder zicht is op het aantal datalekken.

3. Kwaliteits- en ambitieniveaus

Aan de Raad wordt verzocht in te stemmen met de voorgestelde kwaliteits- en ambitieniveaus ten aanzien van privacy. Met de kwaliteitsniveaus wordt aangegeven in welke mate de Rechtspraak op dit moment voldoet aan de implementatie van de privacywet- en regelgeving. De ambitieniveaus geven aan waar de Rechtspraak naartoe streeft. In het borgingsplan is steeds aangegeven wie welke acties moet nemen om tot het voorgestelde ambitieniveau te komen.

De scoring van de kwaliteits- en ambitieniveaus zijn gebaseerd op de KPI's die door het ministerie van Justitie en Veiligheid in het kader van privacymanagement zijn opgesteld. De Rechtspraak heeft naar aanleiding van de pilot die JenV-breed is uitgevoerd, gekozen dit instrumentarium te gebruiken om de borging van privacy op gestructureerde wijze intern te rapporteren.

Totstandkoming niveaus

De beoordeling vindt plaats aan de hand van cijfers op een schaal van 1 tot en met 5, waarbij het getal 1 het laagst is en getal 5 het hoogst. De scoring is zodanig ingericht dat bij score 1 al wordt voldaan aan de eisen uit de privacywet- en regelgeving. Het is dan ook niet de bedoeling om steeds voor alle KPI's te streven naar het cijfer 5. De organisatie bepaalt zelf welk niveau wordt nagestreefd en hoe de organisatie dat niveau bereikt. Hiermee wordt ervoor gezorgd dat iedere organisatie een passende ontwikkeling doormaakt.

De niveaus kennen op hoofdlijnen dezelfde structuur:

5 – voor de betreffende KPI hanteert de organisatie optimale bij de organisatie passende werkvormen om te waarborgen dat blijvend aan de KPI wordt voldaan.
4 – de organisatie hanteert modellen en werkprocessen om de KPI te borgen.
3 – er is centraal inzicht in de KPI.
2 – de organisatie voldoet structureel aan de KPI.
1 – de organisatie voldoet incidenteel aan de KPI.

Als voldaan wordt aan niveau 3, wordt verondersteld dat ook voldaan is aan niveaus 1 en 2. Het hoogste niveau is voor de Rechtspraak steeds het uitgangspunt zolang dit niveau realistisch en passend is. Een dergelijk streven is ook niet onrealistisch en onhaalbaar. Voor enkele KPI's is het ambitieniveau vooralsnog echter lager ingestoken omdat een hogere ambitie niet passend is of om de beoogde groei op een realistische wijze vorm te geven. Wat dat betekent, volgt na onderstaande tabel.

Voorgestelde kwaliteits- en ambitieniveaus

In onderstaande tabel wordt per KPI aangegeven wat het kwaliteits- en ambitieniveau is en welke actie(s) nodig zijn om tot het ambitieniveau te komen.

Key performance indicator	Kwaliteits-niveau	Ambitie-niveau	Actie(s)
1. Privacybeleid	4	5	• Uit het overkoepelend beleid blijkt dat zorgvuldige omgang met persoonsgegevens een kernwaarde van de Rechtspraak. • Implementatie en concretisering van de BIO door IVO Rechtspraak (eind Q2 begin Q3 2022).
2. Register van verwerkings-activiteiten	3	5	Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).
3. Aantonen toestemming	2	3	• Opstellen en bijwerken van de registers van verwerkingsactiviteiten (continu, alle gerechten en landelijke diensten). • Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).
4. Registratie van datalekken	4	5	• Afspraken uniforme melding datalekken (LOBRO; eind 4e kwartaal 2022). • Experiment en landelijke uitrol anonimiseertool (projectleider anonimisering bij IVO; uitrol van de anonimiseertool begint – onder voorwaarden – in 2022).

			• Aanpassen digitale postkamer om datalekken te verminderen. (Projectteams DT en DZD van IVO; beoogde update begin 2023).
5. Verwerkingen door verwerkers	4	5	• Opvragen status verwerkersovereenkomsten/privacyafspraken (beleidsmedewerker privacy, Q2 2022). • Afsluiten nog ontbrekende verwerkersovereenkomsten/privacyafspraken (dienstenmanagers IVO, SP&K monitort). • Borgen periodieke evaluatie en actualisatie verwerkersovereenkomsten/privacyafspraken (Privacy officer/ Adviseur privacy en informatiebeveiliging, Q4 2022).
6. Gezamenlijke verantwoordelijkheid	3	3	Geen acties noodzakelijk
7. Doorgifte van persoonsgegevens buiten de EER	3	5	Afsluiten en actualiseren verwerkersovereenkomsten met leveranciers die persoonsgegevens in de VS opslaan (IVO Rechtspraak).
8. Privacy by design & privacy by default	2	3	Verder implementeren van privacy by design bij IVO Rechtspraak en gerechten door o.a. het uitvoeren van PIA's en het bijwerken van het register van verwerkingsactiviteiten voorafgaand aan de start van een verwerking (continu).
9. Privacy impact assessments	2	5	• Vaststellen mandateringsstructuur PIA (Adviseur privacy & informatiebeveiliging, Q4 2022). • Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).
10. Waarborgen passend beveiligingsniveau[1]	n.v.t.	n.v.t.	• Opstellen planning verbeteringen IT-systemen (IVO Rechtspraak Q2 2022). • Structurele communicatieaanpak privacy en informatiebeveiliging (IVO Rechtspraak, zie ook punt 8).

[1] Deze KPI staat niet in het privacymanagement KPI's van het ministerie. Op basis van de ervaringen met de eerdere versies van de KPI's is ervoor gekozen deze KPI specifiek toe te voegen voor de Rechtspraak om aan hieraan extra aandacht te besteden.

			• Opstellen beleidslijn bewaartermijnen niet-zaaksgebonden persoonsgegevens (Adviseur privacy en informatiebeveiliging, Q4 2022). • Wegwerken auditbevindingen (IVO Rechtspraak, SP&K monitort). • Vaststellen en implementeren loggingsbeleid (IVO Rechtspraak). • Ontwikkelen centrale loggingsvoorziening (IVO Rechtspraak)
11. Informeren van betrokkenen	3	5	Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).
12. Rechten van betrokkenen	5	5	• Herzien aanvraagformulier op rechtspraak.nl/privacy als onderdeel van structurele kwaliteitsverbetering.
13. Bewustzijn omtrent privacy en opleidingen	2	3	• Vergroten privacybewustzijn (alle gerechten en landelijke diensten, continu) • Implementatie van bewustwordingstool als onderdeel van de BIO.[2]

De KPI's waarvoor is gekozen om het ambitieniveau nog niet op 5 voor te stellen, worden hieronder toegelicht.

- Aantonen toestemming (ambitieniveau 3): de grondslag toestemming wordt binnen de Rechtspraak slechts beperkt gebruikt. Betrokkenen hebben het recht om de toestemming op ieder moment in te trekken. Dat maakt toestemming een ongeschikte verwerkingsgrondslag voor de Rechtspraak. Gebruik van toestemming als grondslag is beperkt tot innovatie in de rechtspraak, zoals Wijkrechtspraak en Uniform Hulp Aanbod (UHA), en bedrijfsvoeringsprocessen, zoals het bijhouden van verjaardagen. Volgens de KPI's van JenV zijn nog twee stappen mogelijk, maar deze hebben vooralsnog niet de hoogste prioriteit of kosten meer dan ze opleveren. Het gaat dan om:
    - inrichten van lokale werkprocessen om de registratie van toestemming te controleren en te actualiseren. Iedere verwerking waarin toestemming wordt gebruikt is anders waardoor uniformering lastig wordt. Landelijke uniformering is beoogd met een kader dat aan de beveiligingscoördinatoren is verstrekt.
    - (elektronische) werkvormen om het verlenen en intrekken van toestemming te registreren. De verwachte voordelen van deze stappen ten opzichte van de kosten zijn beperkt, omdat toestemming beperkt als grondslag wordt gebruikt.

[2] IVO Rechtspraak werkt op het moment van schrijven aan een systeem dat aan de behoefte moet voldoen. De leden van het SBO hebben aangegeven dat ze bij de landelijke implementatie van dit systeem gezamenlijk willen optrekken. Dat zal plaatsvinden als IVO positieve ervaringen heeft met het systeem.

- Gezamenlijk verantwoordelijkheid (ambitieniveau 3): van gezamenlijke verwerkings-verantwoordelijkheid is alleen sprake in de samenwerking tussen de Raad en de gerechten. In dat kader zijn op centraal niveau de taken en bevoegdheden vastgelegd in de privacy governance. Voor een hoger niveau is vanuit de KPI's vereist dat:
    - modellen en werkprocessen worden gebruikt om relaties met gezamenlijke verwerkingsverantwoordelijkheden en de registratie te actualiseren (ambitieniveau 4);
    - voor de Rechtspraak optimaal passende werkvormen worden gebruikt om de governance te evalueren en te actualiseren (ambitieniveau 5).

  Aangezien slechts in één geval sprake is gezamenlijke verwerkingsverantwoordelijkheid worden dergelijke middelen niet noodzakelijk geacht om de governance actueel te houden. De governance wordt in plaats daarvan actueel gehouden door overleg tussen de privacyexperts van de gerechten, IVO Rechtspraak en het bureau Raad.

- Privacy by design en privacy by default (ambitieniveau 3): het gaat hier om een tijdelijke eerste stap. Op dit moment wordt pas geïnventariseerd welke privacymaatregelen noodzakelijk zijn als de voorbereidingen al in een vergevorderd stadium zijn of de verwerking reeds is gestart. Daarnaast ontbreekt nog een proces waarin de bescherming van persoonsgegevens continu wordt verbeterd. De Rechtspraak maakt stappen, maar om een realistische ambitie te formuleren is niveau 3 voorgesteld.

  In de toekomst kan het ambitieniveau worden verhoogd naar 4 of 5. Voor die stappen is vereist dat de naleving van de aantoonbare zorgvuldige omgang en het aantoonbare privacyvriendelijke aanbod aan betrokkene wordt gemonitord (4) en dat hiervoor optimale en passende werkvormen zijn (5). Vooralsnog blijven deze stappen buiten beschouwing om acties goed te kunnen focussen en de onderwerpen gestructureerd te laten groeien.

- Bewustzijn omtrent privacy en opleidingen (ambitieniveau 3): ambitieniveaus 4 en 5 vereisen dat werkprocessen worden ingericht om het privacybewustzijn te verhogen resp. dat er een optimaal voor de organisatie passend en door het hoger management gesteund programma is dat periodiek wordt geëvalueerd.

  Op dit moment bevordert de Rechtspraak het privacybewustzijn structureel (niveau 2). Tegelijkertijd is er nog geen centraal zicht in het niveau van het privacybewustzijn (niveau 3). Dergelijk inzicht is wel noodzakelijk om goede werkprocessen en een goed programma te kunnen formuleren. Vandaar dat de eerste ambitie is om centraal inzicht te krijgen in het niveau van privacybewustzijn. Dat zal nog enige tijd kosten. Zodra dat is gebeurd, kan de Rechtspraak groeien in haar ambitie.

Afgestemd

Het borgingsplan is afgestemd met de leden van de werkgroep privacy[3]. Daarnaast is het document op 29 maart 2022 besproken in het MT Raad.

Bijlage:

- Achtste borgingsplan privacy.

[3] Zie pagina 6 van het borgingsplan.

Deelbesluit 10 - Datalekken
Document 346

de Rechtspraak

aan	SBO
van	[redacted]
datum	23 mei 2022
bijlage(n)	1
onderwerp	Achtste borgingsplan Rechtspraak

Toelichtende notitie achtste borgingsplan:

Stand van zaken ten aanzien van privacy binnen de Rechtspraak tot 1 februari 2022

Inleiding

In het Strategisch Plan Privacy is als algemeen uitgangspunt geformuleerd dat er te allen tijde in overeenstemming met de privacywet- en regelgeving wordt gehandeld. Dit waarborgt een zorgvuldige gegevensverwerking. Hierbij moet steeds een afweging gemaakt worden tussen het belang van privacy en andere belangen, zoals de openbaarheid van de Rechtspraak.

De Rechtspraak is echter nog niet zo ver dat te allen tijde in overeenstemming met de privacywet- en regelgeving wordt gehandeld. Het borgingsplan maakt inzichtelijk waar de Rechtspraak ten aanzien van dit uitgangspunt staat, waar de Rechtspraak naartoe wil en welke activiteiten ondernomen moeten worden om het gat hiertussen te overbruggen. Deze activiteiten beogen niet alleen te voldoen aan de verplichtingen van de Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG (UAVG), maar ook aan de verplichtingen die voortvloeien uit de Wet justitiële en strafvorderlijke gegevens (Wjsg) en bijbehorende regelgeving.

Het borgingsplan is voor het eerst opgesteld ter afronding van het Project AVG van het Bureau Raad op 25 mei 2018. Inmiddels ligt de achtste versie van het document voor.

Scope van het borgingsplan

Het borgingsplan is primair gericht op gegevensverwerkingen door de Raad en IVO Rechtspraak, omdat de meeste privacymaatregelen daar moeten worden genomen. Desalniettemin hebben de gerechtsbesturen ook de verantwoordelijkheid om privacy op lokaal niveau te waarborgen en hierover te rapporteren. Waar mogelijk geeft het borgingsplan een beeld over de mate waarin de gerechten de privacywet- en regelgeving hebben geïmplementeerd. Hiervoor wordt gebruik gemaakt van de uitvragen die plaatsvinden via het Key Control Dashboard en gesprekken met beveiligings- en privacycoördinatoren.

Doel

Het achtste borgingsplan betreft de stand van zaken tot 1 februari 2022. Met dit borgingsplan wordt de Raad geïnformeerd over de stand van zaken betreffende de implementatie van de AVG, UAVG en Wjsg (paragrafen 1 en 2).

Daarnaast wordt het SBO verzocht kennis te nemen van de voorgestelde kwaliteits- en ambitieniveaus. De hiervoor benodigde acties zijn reeds geïnventariseerd en belegd (paragraaf 3).

1. Beeld Rechtspraak

Tot het zesde borgingsplan (1 februari 2021) werd in het borgingsplan gerapporteerd dat de Rechtspraak in control was. Sinds het zesde borgingsplan – en ook nu - wordt geconcludeerd dat de Rechtspraak niet volledig in control of compliant is met de geldende privacywet- en regelgeving.

Met in control wordt bedoeld dat nog niet op alle onderdelen aan de geldende privacywet- en regelgeving wordt voldaan, maar dat wel duidelijk is wanneer hieraan zal worden voldaan. Met compliant wordt bedoeld dat alle aan onderdelen van de privacywet- en regelgeving wordt voldaan en dat de onderdelen zijn geborgd. Hierbij moet de kanttekening gemaakt worden dat nooit sprake kan zijn van 100% compliancy.

2. Ontwikkelingen sinds 1 februari 2022

De peildatum van het achtste borgingsplan is 1 februari. Sindsdien hebben de ontwikkelingen niet stilgestaan. Vier ontwikkelingen worden hieronder uitgelicht:

1. Verbeteringen van de informatievoorziening in het kader van de privacywet- en regelgeving

Sinds het zesde borgingsplan heeft de Raad meermaals met de directie van IVO Rechtspraak gesproken over de verbeteringen in het IT-landschap, de bijbehorende planning en de eventuele acceptatie van risico's. Een overleg over dit onderwerp heeft voor het laatst plaatsgevonden tijdens de Raadsvergadering van 16 februari 2022. Door de directie van IVO Rechtspraak is een notitie ingebracht inzake de huidige stand van zaken van de AVG en Wjsg bij IVO Rechtspraak.

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

Tijdens de Raadsvergadering op 13 april 2022 heeft IVO Rechtspraak de risico's uiteengezet en de planning besproken. Daarnaast wordt een risicobeheersingswerkgroep opgesteld. Het borgingsplan zal bij herijking in juli 2022 hierop worden aangepast.

2. Beleidslijn bewaartermijnen van persoonsgegevens ten behoeve van niet-zaaksgebonden processen en systemen

Verder is in opdracht van het Bureau BVA een onderzoek uitgevoerd naar de bewaartermijnen van persoonsgegevens in niet-zaaksgebonden processen en systemen. De resultaten van dit onderzoek moeten leiden tot een eerste beleidslijn die aansluit op de beleidslijn bewaren van persoonsgegevens in

primaire processystemen. Dit laatste document is besproken in de SBO-vergadering van 14 februari 2022.

De beleidslijn bewaartermijnen van persoonsgegevens in niet-zaaksgebonden processen en systemen is ter eerste consultatie verstuurd naar [redacted], [redacted], [redacted] en [redacted]

3. Herziening Wjsg/Wpg

Begin maart 2022 is het Bureau Raad geïnformeerd over de beëindiging van de herziening van de Wet justitiële en strafvorderlijke gegevens en de Wet politiegegevens. De verantwoordelijke minister heeft hiervoor gekozen, omdat het regeerakkoord niet voorziet in de benodigde financiering van het project. Mocht op een later moment toch een probleem geconstateerd worden, dan wordt binnen de financiële kaders naar een oplossing gezocht.

4. Verbeteringen naar aanleiding van adresseringsfouten via de digitale postkamer

Begin februari 2022 zijn rechtbanken geïnformeerd dat in de periode 10 februari 2020 tot 25 januari 2022 3153 zijn geweest die kunnen worden aangeduid als datalek. Deze datalekken werden veroorzaakt door foutieve adressering via de digitale postkamer. Sindsdien is nader onderzoek gedaan en zijn technische en organisatorische maatregelen doorgevoerd. Hierdoor vinden de datalekken slechts sporadisch plaats. In de gevallen dat datalekken plaatsvinden, gaat het om een fout van een nieuwe medewerker.

Gezien de overwegingen van de product owner digitale postkamer en het kleine aantal meldingen sinds de reeds geïmplementeerde maatregelen, lijken aanvullende technische maatregelen op dit moment niet noodzakelijk. Bij de rechtbanken wordt nogmaals aangegeven hoe belangrijk melden in Classbase is, zodat eerder zicht is op het aantal datalekken.

3. Kwaliteits- en ambitieniveaus

Aan het SBO wordt verzocht kennis te nemen van de voorgestelde kwaliteits- en ambitieniveaus ten aanzien van privacy. Met de kwaliteitsniveaus wordt aangegeven in welke mate de Rechtspraak op dit moment voldoet aan de implementatie van de privacywet- en regelgeving. De ambitieniveaus geven aan waar de Rechtspraak naartoe streeft. In het borgingsplan is steeds aangegeven wie welke acties moet nemen om tot het voorgestelde ambitieniveau te komen.

De scoring van de kwaliteits- en ambitieniveaus zijn gebaseerd op de KPI's die door het ministerie van Justitie en Veiligheid in het kader van privacymanagement zijn opgesteld. De Rechtspraak heeft naar aanleiding van de pilot die JenV-breed is uitgevoerd, gekozen dit instrumentarium te gebruiken om de borging van privacy op gestructureerde wijze intern te rapporteren.

Totstandkoming niveaus

De beoordeling vindt plaats aan de hand van cijfers op een schaal van 1 tot en met 5, waarbij het getal 1 het laagst is en getal 5 het hoogst. De scoring is zodanig ingericht dat bij score 1 al wordt voldaan aan de eisen uit de privacywet- en regelgeving. Het is dan ook niet de bedoeling om steeds voor alle KPI's te streven naar het cijfer 5. De organisatie bepaalt zelf welk niveau wordt nagestreefd en hoe de organisatie dat niveau bereikt. Hiermee wordt ervoor gezorgd dat iedere organisatie een passende ontwikkeling doormaakt.

De niveaus kennen op hoofdlijnen dezelfde structuur:

5 – voor de betreffende KPI hanteert de organisatie optimale bij de organisatie passende werkvormen om te waarborgen dat blijvend aan de KPI wordt voldaan.
4 – de organisatie hanteert modellen en werkprocessen om de KPI te borgen.
3 – er is centraal inzicht in de KPI.
2 – de organisatie voldoet structureel aan de KPI.
1 – de organisatie voldoet incidenteel aan de KPI.

Als voldaan wordt aan niveau 3, wordt verondersteld dat ook voldaan is aan niveaus 1 en 2. Het hoogste niveau is voor de Rechtspraak steeds het uitgangspunt zolang dit niveau realistisch en passend is. Een dergelijk streven is ook niet onrealistisch en onhaalbaar. Voor enkele KPI's is het ambitieniveau vooralsnog echter lager ingestoken omdat een hogere ambitie niet passend is of om de beoogde groei op een realistische wijze vorm te geven. Wat dat betekent, volgt na onderstaande tabel.

Voorgestelde kwaliteits- en ambitieniveaus

In onderstaande tabel wordt per KPI aangegeven wat het kwaliteits- en ambitieniveau is en welke actie(s) nodig zijn om tot het ambitieniveau te komen.

Key performance indicator	Kwaliteits-niveau	Ambitie-niveau	Actie(s)
1. Privacybeleid	4	5	• Uit het overkoepelend beleid blijkt dat zorgvuldige omgang met persoonsgegevens een kernwaarde van de Rechtspraak. • Implementatie en concretisering van de BIO door IVO Rechtspraak (eind Q2 begin Q3 2022).
2. Register van verwerkings-activiteiten	3	5	Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).
3. Aantonen toestemming	2	3	• Opstellen en bijwerken van de registers van verwerkingsactiviteiten (continu, alle gerechten en landelijke diensten).

			• Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).
4. Registratie van datalekken	4	5	• Afspraken uniforme melding datalekken (LOBRO; eind 4e kwartaal 2022). • Experiment en landelijke uitrol anonimiseertool (projectleider anonimisering bij IVO; uitrol van de anonimiseertool begint – onder voorwaarden – in 2022). • Aanpassen digitale postkamer om datalekken te verminderen. (Projectteams DT en DZD van IVO; beoogde update begin 2023).
5. Verwerkingen door verwerkers	4	5	• Opvragen status verwerkersovereenkomsten/privacyafspraken (beleidsmedewerker privacy, Q2 2022). • Afsluiten nog ontbrekende verwerkersovereenkomsten/privacyafspraken (dienstenmanagers IVO, SP&K monitort). • Borgen periodieke evaluatie en actualisatie verwerkersovereenkomsten/privacyafspraken (Privacy officer/ Adviseur privacy en informatiebeveiliging, Q4 2022).
6. Gezamenlijke verantwoordelijkheid	3	3	Geen acties noodzakelijk
7. Doorgifte van persoonsgegevens buiten de EER	3	5	Afsluiten en actualiseren verwerkersovereenkomsten met leveranciers die persoonsgegevens in de VS opslaan (IVO Rechtspraak).
8. Privacy by design & privacy by default	2	3	Verder implementeren van privacy by design bij IVO Rechtspraak en gerechten door o.a. het uitvoeren van PIA's en het bijwerken van het register van verwerkingsactiviteiten voorafgaand aan de start van een verwerking (continu).
9. Privacy impact assessments	2	5	• Vaststellen mandateringsstructuur PIA (Adviseur privacy & informatiebeveiliging, Q4 2022). • Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).

10. Waarborgen passend beveiligingsniveau[1]	n.v.t.	n.v.t.	• Opstellen planning verbeteringen IT-systemen (IVO Rechtspraak Q2 2022). • Structurele communicatieaanpak privacy en informatiebeveiliging (IVO Rechtspraak, zie ook punt 8). • Opstellen beleidslijn bewaartermijnen niet-zaaksgebonden persoonsgegevens (Adviseur privacy en informatiebeveiliging, Q4 2022). • Wegwerken auditbevindingen (IVO Rechtspraak, SP&K monitort). • Vaststellen en implementeren loggingsbeleid (IVO Rechtspraak). • Ontwikkelen centrale loggingsvoorziening (IVO Rechtspraak)
11. Informeren van betrokkenen	3	5	Implementatie van SmartPIA (samenwerking Bureau Raad en IVO, Q1 en Q2 2022).
12. Rechten van betrokkenen	5	5	• Herzien aanvraagformulier op rechtspraak.nl/privacy als onderdeel van structurele kwaliteitsverbetering.
13. Bewustzijn omtrent privacy en opleidingen	2	3	• Vergroten privacybewustzijn (alle gerechten en landelijke diensten, continu) • Implementatie van bewustwordingstool als onderdeel van de BIO.[2]

De KPI's waarvoor is gekozen om het ambitieniveau nog niet op 5 voor te stellen, worden hieronder toegelicht.

- Aantonen toestemming (ambitieniveau 3): de grondslag toestemming wordt binnen de Rechtspraak slechts beperkt gebruikt. Betrokkenen hebben het recht om de toestemming op ieder moment in te trekken. Dat maakt toestemming een ongeschikte verwerkingsgrondslag voor de Rechtspraak. Gebruik van toestemming als grondslag is beperkt tot innovatie in de rechtspraak, zoals Wijkrechtspraak en Uniform Hulp Aanbod (UHA), en bedrijfsvoeringsprocessen, zoals het bijhouden van verjaardagen. Volgens de KPI's van JenV zijn nog twee stappen mogelijk, maar deze hebben vooralsnog niet de hoogste prioriteit of kosten meer dan ze opleveren. Het gaat dan om:

[1] Deze KPI staat niet in het privacymanagement KPI's van het ministerie. Op basis van de ervaringen met de eerdere versies van de KPI's is ervoor gekozen deze KPI specifiek toe te voegen voor de Rechtspraak om aan hieraan extra aandacht te besteden.

[2] IVO Rechtspraak werkt op het moment van schrijven aan een systeem dat aan de behoefte moet voldoen. De leden van het SBO hebben aangegeven dat ze bij de landelijke implementatie van dit systeem gezamenlijk willen optrekken. Dat zal plaatsvinden als IVO positieve ervaringen heeft met het systeem.

  - inrichten van lokale werkprocessen om de registratie van toestemming te controleren en te actualiseren. Iedere verwerking waarin toestemming wordt gebruikt is anders waardoor uniformering lastig wordt. Landelijke uniformering is beoogd met een kader dat aan de beveiligingscoördinatoren is verstrekt.
  - (elektronische) werkvormen om het verlenen en intrekken van toestemming te registreren. De verwachte voordelen van deze stappen ten opzichte van de kosten zijn beperkt, omdat toestemming beperkt als grondslag wordt gebruikt.

- Gezamenlijk verantwoordelijkheid (ambitieniveau 3): van gezamenlijke verwerkings-verantwoordelijkheid is alleen sprake in de samenwerking tussen de Raad en de gerechten. In dat kader zijn op centraal niveau de taken en bevoegdheden vastgelegd in de privacy governance. Voor een hoger niveau is vanuit de KPI's vereist dat:
  - modellen en werkprocessen worden gebruikt om relaties met gezamenlijke verwerkingsverantwoordelijkheden en de registratie te actualiseren (ambitieniveau 4);
  - voor de Rechtspraak optimaal passende werkvormen worden gebruikt om de governance te evalueren en te actualiseren (ambitieniveau 5).

  Aangezien slechts in één geval sprake is gezamenlijke verwerkingsverantwoordelijkheid worden dergelijke middelen niet noodzakelijk geacht om de governance actueel te houden. De governance wordt in plaats daarvan actueel gehouden door overleg tussen de privacyexperts van de gerechten, IVO Rechtspraak en het bureau Raad.

- Privacy by design en privacy by default (ambitieniveau 3): het gaat hier om een tijdelijke eerste stap. Op dit moment wordt pas geïnventariseerd welke privacymaatregelen noodzakelijk zijn als de voorbereidingen al in een vergevorderd stadium zijn of de verwerking reeds is gestart. Daarnaast ontbreekt nog een proces waarin de bescherming van persoonsgegevens continu wordt verbeterd. De Rechtspraak maakt stappen, maar om een realistische ambitie te formuleren is niveau 3 voorgesteld.

  In de toekomst kan het ambitieniveau worden verhoogd naar 4 of 5. Voor die stappen is vereist dat de naleving van de aantoonbare zorgvuldige omgang en het aantoonbare privacyvriendelijke aanbod aan betrokkene wordt gemonitord (4) en dat hiervoor optimale en passende werkvormen zijn (5). Vooralsnog blijven deze stappen buiten beschouwing om acties goed te kunnen focussen en de onderwerpen gestructureerd te laten groeien.

- Bewustzijn omtrent privacy en opleidingen (ambitieniveau 3): ambitieniveaus 4 en 5 vereisen dat werkprocessen worden ingericht om het privacybewustzijn te verhogen resp. dat er een optimaal voor de organisatie passend en door het hoger management gesteund programma is dat periodiek wordt geëvalueerd.

  Op dit moment bevordert de Rechtspraak het privacybewustzijn structureel (niveau 2). Tegelijkertijd is er nog geen centraal zicht in het niveau van het privacybewustzijn (niveau 3). Dergelijk inzicht is wel noodzakelijk om goede werkprocessen en een goed programma te

kunnen formuleren. Vandaar dat de eerste ambitie is om centraal inzicht te krijgen in het niveau van privacybewustzijn. Dat zal nog enige tijd kosten. Zodra dat is gebeurd, kan de Rechtspraak groeien in haar ambitie.

Afgestemd

Het borgingsplan is afgestemd met de leden van de werkgroep privacy[3]. Daarnaast is het document op 29 maart 2022 besproken in het MT Raad en op 13 april 2022 in de Raadsvergadering.

Bijlage:

- Achtste borgingsplan privacy.

[3] Zie pagina 6 van het borgingsplan.

Deelbesluit 10 - Datalekken
Document 347

WZD verstrekkingen aan CIZ per rechtbank en maand waarbij de externe referentie niet het juiste formaat heeft van CIZ (8 cijfers). Als formaat_referentie="CORV-formaat" dan zijn vermoedelijk stukken uit een jeugdzaak verstrekt. Als formaat_referentie="OM-formaat" dan zijn vermoedelijk stukken uit een WvGGZ verstrekt. Als formaat_referentie=GEEN dan kon er geen externe referentie bepaald worden obv het zaaknummer; wellicht was het zaaknummer verkeerd of was er bij de indiening geen zaaknummer vastgelegd.

rechtbank	formaat_referentie	2021-01	2021-02	2021-03	2021-04	2021-05	2021-06	2021-07	2021-08	2021-09	2021-10	2021-11	2021-12	2022-01	2022-02	2022-03	2022-04
Den Haag	CORV-formaat	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
Limburg	CORV-formaat	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Oost-Brabant	CORV-formaat	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Rotterdam	CORV-formaat	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Amsterdam	GEEN	3	3	2	0	2	1	0	0	0	0	0	0	0	0	0	0
Den Haag	GEEN	0	7	18	45	2	0	0	0	0	0	0	0	0	0	1	0
Gelderland	GEEN	5	2	5	3	1	1	1	2	0	4	0	0	0	0	0	0
Limburg	GEEN	13	21	6	7	2	1	0	0	0	0	0	0	0	0	0	0
Midden-Nederland	GEEN	1	2	5	1	3	0	0	0	0	0	0	0	0	0	0	0
Noord-Holland	GEEN	1	23	0	1	1	0	1	0	0	0	0	0	0	0	0	0
Noord-Nederland	GEEN	4	3	5	0	2	1	0	0	0	1	0	0	0	0	0	0
Oost-Brabant	GEEN	0	4	1	1	1	0	0	0	0	0	0	0	0	0	1	0
Overijssel	GEEN	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0
Rotterdam	GEEN	0	2	6	4	0	1	1	1	0	0	2	0	0	0	0	0
Zeeland-West-Brabant	GEEN	9	7	3	2	0	1	0	0	0	0	0	0	0	1	1	0
Amsterdam	OM-formaat	0	0	2	7	0	0	0	0	0	3	0	0	0	0	0	0
Den Haag	OM-formaat	0	0	0	0	0	2	0	1	0	0	0	0	0	0	1	0
Gelderland	OM-formaat	0	0	0	1	0	0	0	1	0	2	0	3	1	0	1	0
Limburg	OM-formaat	0	1	0	1	0	0	0	0	2	0	0	0	1	0	0	0
Midden-Nederland	OM-formaat	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0
Noord-Holland	OM-formaat	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0
Noord-Nederland	OM-formaat	0	0	0	1	2	1	0	0	0	2	0	2	0	0	0	0
Oost-Brabant	OM-formaat	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0
Overijssel	OM-formaat	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0
Rotterdam	OM-formaat	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
Zeeland-West-Brabant	OM-formaat	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0

WZD verstrekkingen aan IGJ per rechtbank en maand waarbij de externe referentie niet het juiste formaat heeft van CIZ (8 cijfers). Als formaat_referentie="CORV-formaat" dan zijn vermoedelijk stukken uit een jeugdzaak verstrekt. Als formaat_referentie="OM-formaat" dan zijn vermoedelijk stukken uit een WvGGZ verstrekt. Als formaat_referentie=GEEN dan kon er geen externe referentie bepaald worden obv het zaaknummer; wellicht was het zaaknummer verkeerd of was er bij de indiening geen zaaknummer vastgelegd.

rechtbank	formaat_referentie	2021-01	2021-02	2021-03	2021-04	2021-05	2021-06	2021-07	2021-08	2021-09	2021-10	2021-11	2021-12	2022-01	2022-02	2022-03	2022-04
Amsterdam	GEEN	3	3	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Den Haag	GEEN	0	0	0	15	0	0	0	0	0	0	0	0	0	0	0	0
Noord-Holland	GEEN	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Noord-Nederland	GEEN	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Oost-Brabant	GEEN	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Rotterdam	GEEN	0	1	3	1	0	0	0	0	0	0	0	0	0	0	0	0
Amsterdam	OM-formaat	0	0	1	7	0	0	0	0	0	0	0	0	0	0	0	0
Noord-Holland	OM-formaat	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Oost-Brabant	OM-formaat	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0

WvGGZ verstrekkingen aan het OM per rechtbank en maand waarbij de externe referentie niet het juiste formaat heeft van het OM. Als formaat_referentie="CIZ-formaat" dan zijn vermoedelijk stukken uit een WZD verstrekt. Als formaat_referentie="CORV-formaat" dan zijn vermoedelijk stukken uit een jeugdzaak verstrekt. Als formaat_referentie=GEEN dan kon er geen externe referentie bepaald worden obv het zaaknummer; wellicht was het zaaknummer verkeerd of was er bij de indiening geen zaaknummer vastgelegd.

rechtbank	formaat_referentie	2021-01	2021-02	2021-03	2021-04	2021-05	2021-06	2021-07	2021-08	2021-09	2021-10	2021-11	2021-12	2022-01	2022-02	2022-03	2022-04
Amsterdam	CIZ-formaat	0	0	11	5	9	1	1	2	1	0	0	0	0	0	0	0
Den Haag	CIZ-formaat	0	0	3	1	2	3	0	3	3	2	1	0	3	0	0	0
Gelderland	CIZ-formaat	0	0	3	4	3	1	1	1	1	2	1	2	0	0	0	0
Limburg	CIZ-formaat	0	0	0	3	1	1	1	0	1	2	3	0	0	0	1	1
Midden-Nederland	CIZ-formaat	0	4	6	2	2	4	3	1	1	2	0	3	0	0	0	0
Noord-Holland	CIZ-formaat	0	0	1	1	0	1	0	0	1	0	1	1	2	0	0	0
Noord-Nederland	CIZ-formaat	0	0	1	1	0	4	2	1	1	3	2	3	0	0	0	0
Oost-Brabant	CIZ-formaat	0	0	1	2	0	1	0	2	0	0	0	1	0	0	0	0
Overijssel	CIZ-formaat	0	2	1	1	0	0	2	1	0	0	1	1	1	0	0	0
Rotterdam	CIZ-formaat	0	0	0	3	3	1	2	0	5	4	0	1	2	0	0	0
Zeeland-West-Brabant	CIZ-formaat	0	0	0	2	1	0	4	3	0	1	2	1	0	0	0	0
Gelderland	CORV-formaat	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0
Limburg	CORV-formaat	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Midden-Nederland	CORV-formaat	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
Noord-Nederland	CORV-formaat	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Rotterdam	CORV-formaat	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0
Amsterdam	GEEN	0	13	28	26	20	10	0	1	0	1	2	0	0	1	0	0
Den Haag	GEEN	0	110	166	182	35	14	3	0	0	0	0	0	0	0	2	2
Gelderland	GEEN	2	24	21	20	10	13	2	3	0	1	2	0	2	0	2	0
Limburg	GEEN	0	57	47	39	10	8	0	0	0	0	1	0	0	1	0	0
Midden-Nederland	GEEN	7	58	28	18	12	11	12	3	0	0	0	1	0	0	0	0
Noord-Holland	GEEN	1	62	16	9	12	9	5	1	0	0	0	0	1	1	0	0
Noord-Nederland	GEEN	7	19	17	8	5	11	6	9	3	1	1	0	0	1	0	0
Oost-Brabant	GEEN	0	1	11	13	7	3	0	0	0	0	2	0	0	0	0	0
Overijssel	GEEN	0	9	10	8	6	3	1	1	0	0	0	0	0	0	0	0
Rotterdam	GEEN	4	57	29	18	11	22	5	5	1	2	3	6	4	1	0	0
Zeeland-West-Brabant	GEEN	17	5	13	17	8	9	5	2	0	1	0	0	0	1	1	0

WvGGZ verstrekkingen aan IGJ per rechtbank en maand waarbij de externe referentie niet het juiste formaat heeft van het OM. Als formaat_referentie="CIZ-formaat" dan zijn vermoedelijk stukken uit een WZD verstrekt. Als formaat_referentie="CORV-formaat" dan zijn vermoedelijk stukken uit een jeugdzaak verstrekt. Als formaat_referentie=GEEN dan kon er geen externe referentie bepaald worden obv het zaaknummer; wellicht was het zaaknummer verkeerd of was er bij de indiening geen zaaknummer vastgelegd.

rechtbank	formaat_referentie	2021-01	2021-02	2021-03	2021-04	2021-05	2021-06	2021-07	2021-08	2021-09	2021-10	2021-11	2021-12	2022-01	2022-02	2022-03	2022-04
Amsterdam	CIZ-formaat	0	0	11	5	9	1	1	2	1	0	0	0	0	0	0	0
Den Haag	CIZ-formaat	0	0	0	1	2	3	0	3	3	2	1	0	3	0	1	0
Gelderland	CIZ-formaat	0	0	3	4	3	1	0	0	1	1	0	2	0	0	0	0
Limburg	CIZ-formaat	0	0	0	0	0	0	0	0	0	0	3	0	0	0	1	0
Midden-Nederland	CIZ-formaat	1	0	2	1	2	3	3	1	1	2	0	3	0	0	0	0
Noord-Holland	CIZ-formaat	0	0	1	1	0	1	0	0	1	0	1	1	2	0	0	0
Noord-Nederland	CIZ-formaat	0	0	0	1	0	0	2	1	0	1	0	0	0	0	0	0
Oost-Brabant	CIZ-formaat	0	0	1	2	0	1	0	1	0	0	0	1	0	0	0	0
Overijssel	CIZ-formaat	0	1	0	0	1	0	3	1	0	0	1	1	0	0	0	0
Rotterdam	CIZ-formaat	0	1	0	1	2	1	2	0	5	4	0	1	2	0	0	0
Zeeland-West-Brabant	CIZ-formaat	1	0	0	2	1	0	4	3	0	1	2	1	0	0	0	0
Gelderland	CORV-formaat	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0
Limburg	CORV-formaat	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Midden-Nederland	CORV-formaat	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
Rotterdam	CORV-formaat	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0
Amsterdam	GEEN	0	13	28	26	20	8	0	1	0	1	2	0	0	0	0	0
Den Haag	GEEN	0	0	1	135	32	13	0	0	1	0	0	1	0	0	0	2
Gelderland	GEEN	224	93	22	20	10	12	2	3	0	0	0	0	2	0	2	0
Midden-Nederland	GEEN	0	1	9	7	5	11	4	3	0	0	0	1	0	0	0	0
Noord-Holland	GEEN	0	47	30	10	10	8	0	1	0	0	0	0	0	1	0	0
Noord-Nederland	GEEN	43	13	6	3	2	8	3	0	1	2	1	0	0	0	0	0
Oost-Brabant	GEEN	0	1	12	13	7	7	0	0	0	0	0	0	0	0	0	0
Overijssel	GEEN	0	12	5	1	4	2	0	1	0	0	0	0	0	0	0	0
Rotterdam	GEEN	24	16	31	18	13	22	5	3	1	2	3	6	4	1	0	0
Zeeland-West-Brabant	GEEN	99	35	15	19	9	7	4	2	0	1	0	0	0	2	1	0

Jeugd verstrekkingen aan een CORV-partij per rechtbank en maand waarbij de externe referentie niet een juist formaat heeft van CORV. Als formaat_referentie="CIZ-formaat" dan zijn vermoedelijk stukken uit een WZD-zaak verstrekt. Als formaat_referentie="OM-formaat" dan zijn vermoedelijk stukken uit een WvGGZ-zaak verstrekt. Als formaat_referentie=GEEN dan kon er geen externe referentie bepaald worden obv het zaaknummer; wellicht was het zaaknummer verkeerd of was er bij de indiening geen zaaknummer vastgelegd. Deze verstrekkingen zijn aan een CORV-partij gestuurd. Opmerking: er waren ook verstrekkingen waarbij als zaaknummer "N.V.T." is gevuld; hierbij had de externe referentie een afwijkend formaat zoals zaaknummer, naam, indieningnummer; deze zijn uit dit overzicht gelaten.

rechtbank	formaat_referentie	2021-01	2021-02	2021-03	2021-04	2021-05	2021-06	2021-07	2021-08	2021-09	2021-10	2021-11	2021-12	2022-01	2022-02	2022-03	2022-04
Gelderland	CIZ-formaat	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0
Noord-Holland	CIZ-formaat	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Noord-Nederland	CIZ-formaat	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0
Zeeland-West-Brabant	CIZ-formaat	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
Amsterdam	GEEN	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0
Den Haag	GEEN	0	0	0	4	6	20	12	4	4	2	2	2	5	2	0	0
Gelderland	GEEN	0	0	0	1	29	17	17	4	5	3	1	0	2	2	2	2
Limburg	GEEN	0	0	0	0	0	6	3	3	2	2	0	2	0	1	0	0
Midden-Nederland	GEEN	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0
Noord-Holland	GEEN	0	0	0	5	12	45	1	0	0	0	1	0	0	0	0	0
Noord-Nederland	GEEN	0	0	0	0	0	3	0	1	2	2	2	33	0	0	2	0
Oost-Brabant	GEEN	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0
Overijssel	GEEN	0	0	0	0	5	5	4	3	4	9	4	4	0	4	3	0
Rotterdam	GEEN	18	9	13	15	9	20	0	2	1	2	2	1	2	3	3	1
Zeeland-West-Brabant	GEEN	0	0	0	0	0	0	0	0	0	0	0	2	0	2	4	0
Gelderland	OM-formaat	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
Midden-Nederland	OM-formaat	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Noord-Holland	OM-formaat	0	0	0	1	5	0	0	0	0	0	0	0	0	0	0	0
Overijssel	OM-formaat	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0

Deelbesluit 10 - Datalekken
Document 348

de Rechtspraak

aan Voorzitter en leden Raad voor de rechtspraak
Voorzitter en leden PRO
Voorzitter en leden Gerechtsbesturen
cc MT bureau Raad
Strategisch Bedrijfsvoeringsoverleg (SBO)
van [redacted]
datum 28 februari 2018
onderwerp Voortgang implementatie AVG en Richtlijn

Notitie voortgang implementatie AVG en Richtlijn

Samenvatting
Deze notitie beschrijft de voortgang van het project implementatie AVG en Richtlijn om u daarover te informeren. Het project levert op drie deelgebieden producten op: een kader governance en toezicht, een landelijk register van verwerkingen en gegevensbeschermingsbeleid, -procedures en -handreikingen. Daarnaast draagt het project zorg voor een intern en extern communicatieplan en voor actieplannen met verbeteraanbevelingen met betrekking tot de uitvoering van privacyregels.

De nieuwe wet- en regelgeving welke in mei van toepassing wordt, verschilt materieelrechtelijk wel enigszins maar niet wezenlijk van de huidige basisregels zoals opgenomen in de Wet bescherming persoonsgegevens (Wbp).Wat wel cruciaal is, is de in de AVG en de Richtlijn opgenomen verantwoordingsplicht voor organisaties. Deze verantwoordingsplicht houdt in dat organisaties moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG en de Richtlijn te voldoen. Het project implementatie AVG/Richtlijn beoogt dan ook in belangrijke mate om de gerechten en landelijke diensten aan die verantwoordingsplicht te kunnen laten voldoen.

Van de gerechtsbesturen en directies landelijke diensten wordt in het kader van de implementatie het volgende gevraagd:
- Mandatering van het PRO om namens de gerechten te besluiten omtrent het beleidskader governance en toezicht, het gegevensbeschermingsbeleid en de privacyverklaring van de Rechtspraak.
- In de periode van 13 maart tot 28 april: invullen van het modelverwerkingenregister om de lokale gegevensverwerkingen in kaart te brengen.
- Na 28 april: aanpassen van lokale werkprocessen aan de hand van te verstrekken checklists.
- Na 14 mei: aanpassen autorisatiematrices.

Van de gerechtsbesturen (door middel van mandatering van) het PRO wordt het volgende gevraagd:
- Op 9 april: instemming met het beleidskader governance en toezicht.
- Op 14 mei: instemming met het gegevensbeschermingsbeleid en de privacyverklaring van de rechtspraak.

Het overall beeld is dat dankzij de inspanning van velen de Rechtspraak op tijd zal kunnen beschikken over de instrumenten om de AVG en de Richtlijn na te leven.

Inleiding
Op 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Voor het strafrecht is er de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn) die voor 06 mei vertaald wordt in Nederlandse wetgeving door aanpassingen van de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). De nieuwe wet- en regelgeving welke in mei van toepassing wordt, verschilt materieelrechtelijk wel enigszins, maar niet wezenlijk van de huidige basisregels zoals opgenomen in de Wet bescherming persoonsgegevens (Wbp). Wat wel cruciaal is, is de in de AVG en de Richtlijn opgenomen verantwoordingsplicht voor organisaties. Deze verantwoordingsplicht houdt in dat organisaties moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG en de Richtlijn te voldoen. Het project implementatie AVG/Richtlijn beoogt dan ook in belangrijke mate om de gerechten en diensten aan die verantwoordingsplicht te kunnen laten voldoen.

Projectdoelstelling.
De projectdoelstelling is ervoor te zorgen dat de Rechtspraak in staat wordt gesteld aan te tonen dat de naleving van de AVG en de Richtlijn is geborgd. De projectdoelstelling wordt gerealiseerd door de volgende kaders te realiseren die aan de gerechten en landelijke diensten ter beschikking worden gesteld ten behoeve van lokale implementatie:

1. Governance en toezicht;
2. Register van verwerkingen;
3. Gegevensbeschermingsbeleid, procedures en handreikingen;

De kaders worden gebaseerd op bestaande organisatiestructuren, processen en systemen.
De implementatie wordt waar mogelijk centraal ingevuld. Gerechten en diensten krijgen medio maart instructie voor het uitvoeren van specifieke lokale inventarisaties. Bevindingen die bij landelijk en lokale inventarisaties worden geconstateerd, worden in de actieplannen opgenomen. De actieplannen worden voorzien van een risico- en belangenafweging en een tijdspad. Uit een risico- en belangenafweging kan ook voortkomen dat acties na 25 mei kunnen worden opgepakt. Dit zal met name het geval zijn voor bepaalde technische of zeer arbeidsintensieve aanpassingen.

Projectorganisatie.
In september 2017 is het Strategisch plan privacy vastgesteld. Daarin is vermeld dat dit plan in opdracht van de portefeuillehouder van de Raad door een projectteam van het bureau Raad zal worden geïmplementeerd. Dit projectteam onder leiding van de projectleider [redacted], ondersteund door een privacy adviseur en een communicatie adviseur, is sinds november bezig de implementatie voor te bereiden. Het projectteam werkt nauw samen met de functionaris gegevensbescherming en de landelijk beveiligingsambtenaar. Het projectteam wordt ondersteund door een team van juridisch en technisch adviseurs vanuit de Raad en de landelijke diensten. De projectresultaten worden gerealiseerd in samenwerking en overleg met de landelijke diensten en de gerechten. In dat kader zijn projectgroepen opgericht welke verantwoordelijk zijn voor de oplevering van deelresultaten.

Projectcommunicatie.
Ieder gerecht en dienst heeft een contactpersoon privacy die voor de eigen organisatie en voor het projectteam als aanspreekpunt fungeert. Aanspreekpunten zijn over het algemeen beveiligingscoördinatoren en soms bestuurssecretarissen. Zij worden geïnformeerd over de voortgang van het implementatieproject onder meer tijdens landelijke themamiddagen. De eerste was op 23 januari jl. De volgende is op 13 maart a.s. De derde zal medio april plaatsvinden. Verder verloopt communicatie via landelijke gremia zoals de vakgroep HRM en het LOBRO. Eind februari zal een landelijke intropagina en teamsite voor contactpersonen worden opgericht.

Tijdpad

Begin maart	Modelregister, beleidskaders en actieplannen in concept gereed
13 maart	Tweede themamiddag aanspreekpunten gerechten en diensten
	Aanspreekpunten krijgen instructie voor het uitvoeren van lokale inventarisaties
09 april	**Besluitvorming beleidskader governance en toezicht**
Medio april	Derde themamiddag
28 april	**Landelijk verwerkingsregister gereed**
14 mei	**Besluitvorming beleid gegevensbescherming en privacyverklaring rechtspraak**
25 mei	**Publicatie beleid gegevensbescherming en privacyverklaring op Rechtspraak.nl**
Juni	Eindrapportage en decharge

1. Governance en toezicht

In het beleidskader governance en toezicht staat beschreven hoe de taken, verantwoordelijkheden en bevoegdheden tussen Raad, gerechten en landelijke diensten zijn verdeeld. Daarbij wordt conform het strategisch plan gekozen voor inzet van een landelijke Functionaris Gegevensbescherming, een Privacy Officer bij IVO en aanspreekpunten/Privacy Officers bij de gerechten en overige landelijke diensten. Ook het instrumentarium voor toezicht is beschreven (PDCA, IC, P&V en Auditing). Het beleid governance en toezicht wordt op 28 maart in de Raad en op 9 april in het PRO besproken.

Deelproject	Doelstelling	Afronding
Governance en toezicht	Het beleidskader governance en toezicht wordt vastgesteld door Raad en PRO en ter uitvoering aan de gerechten en diensten ter beschikking gesteld.	09 april ☺

2. Verwerkingsregister

Ingevolge artikel 30 van de AVG en artikel 24 van de Richtlijn zijn organisaties verplicht een verwerkingsregister te houden waarin tenminste het volgende beschreven staat:

- Processen en systemen waarin persoonsgegevens worden verwerkt;
- Per type betrokkene de categorieën persoonsgegevens welke worden verzameld;
- Van welke actoren en op welke wijze persoonsgegevens worden verkregen;
- Aan welke actoren en op welke wijze persoonsgegevens worden verstrekt;
- De doeleinden en grondslagen voor verwerking van persoonsgegevens;
- De organisatorische en technische maatregelen die worden getroffen teneinde de rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens te borgen.

Voor de Rechtspraak wordt onderscheid gemaakt tussen zeven aandachtsgebieden: straf, civiel, bestuursrecht, publieke registers, mediation, personeel en bedrijfsvoering. Ten behoeve van de gerechten en landelijke diensten wordt een modelregister gerealiseerd dat de gerechten en diensten lokaal kunnen invullen. Het modelregister komt 13 maart beschikbaar voor de gerechten en diensten; zij hebben tot 28 april de tijd om het register lokaal te vullen.
Een samenvatting van het register zal worden gepubliceerd op Rechtspraak nl.

Deelproject	Omschrijving	Verwachting
Verwerkingen centrale IT applicaties	Deelproject IVO beschrijft verwerking van persoonsgegevens in 149 centrale IT applicaties. Voortgang: inmiddels zijn 50 van de 149 IT applicaties beschreven en op korte termijn worden meer verwacht.	28 april ☺
Beveiliging centrale IT applicaties	Deelproject IVO beschrijft voor 149 IT applicaties de beveiligingsmaatregelen. Voortgang: een eerste inventarisatie wordt medio maart afgerond. Daarna vindt waar nodig voor bepaalde systemen nader onderzoek plaats.	28 april ☺
Externe IT applicaties	Deelproject IVO brengt koppelvlakken met externe systemen in kaart De inventarisatie van externe systemen dient nog te beginnen. De verwachting is dat dit snel kan worden afgerond. Dit is echter nog niet zeker.	28 april 😑
Model register van lokale verwerkingen	De deelprojectgroep maakt in samenwerking met een pilotgerecht (rechtbank Noord-Holland) een modelregister voor gerechten. Hierbij wordt deels voortgebouwd op de inventarisatie van centrale IT applicaties en dit wordt aangevuld met standaardbeschrijvingen van lokale processen. Denk hierbij aan dossiermanagement, postverwerking, administratie, griffie, bodeloge, archivering, etc. 13 maart: eerste versie modelregister met checklist gereed voor gerechten en diensten.	28 april V2 ☺
Lokale inventarisaties	Gerechten en landelijke diensten inventariseren verwerkingen lokaal aan de hand van het modelregister en instructie vanuit het projectteam.	28 april ☺
Publicatie landelijk register van verwerkingen op Rechtspraak nl	Projectteam publiceert op 25 mei een samenvatting van het landelijk register van verwerkingen op Rechtspraak nl.	25 mei ☺

3. Beleid, procedures en handreikingen

In het gegevensbeschermingsbeleid worden de beginselen van de AVG en de Richtlijn vertaald naar beleidsregels. Deze beginselen staan beschreven in artikel 5 van de AVG en in artikel 6 van de Richtlijn en hebben betrekking op rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid. Het gegevensbeschermingsbeleid vormt een referentiekader voor gegevensbescherming waarbij wordt voortgebouwd op bestaand beleid, procedures en maatregelen.

Deelproject	Omschrijving	Verwachting
Gegevensbeschermings-beleid betrokkenen in rechtszaken	Projectteam stelt het gegevensbeschermingsbeleid op en legt dit ter besluitvorming voor aan Raad en PRO. Het concept beleid wordt afgestemd met aanspreekpunten bij gerechten en diensten en met een adviescommissie van rechters en raadsheren.	14 mei ☺
Gegevensbeschermingsbeleid Rechtspraakmedewerkers en overige bedrijfsvoering	Projectteam stelt het gegevensbeschermingsbeleid op en legt dit ter besluitvorming voor aan Raad en PRO Het concept beleid wordt afgestemd met de Vakgroep HRM en de COR.	14 mei ☺

Checklist bewaren en vernietigen	Projectteam maakt in overleg met de mandaatgroep archieven een lijst met bewaartermijnen als referentiekader voor de gerechten en diensten.	28 april ☺
Ontvangst en verstrekking gegevens externe actoren	Projectteam brengt in samenwerking met het LBVr en de LOV's de wet- en regelgeving in kaart die ten grondslag ligt aan de ontvangst en verstrekking van gegevens van en aan externe actoren.	28 april ☺
Rechten betrokkenen	Het projectteam stelt een landelijke procedure op voor rechten betrokkenen bij bestuur, straf, civiel, personeel en overig. Voor het strafrecht wordt afstemming gezocht met het implementatieteam van het OM.	25 mei ☺
Verwerkersafspraken (marktpartijen)	De Rechtspraak heeft raamcontracten, IT contracten en lokale contracten met externe leveranciers die onder verantwoordelijk-heid van de Rechtspraak persoonsgegevens verwerken. De afspraken over verwerking van persoonsgegevens met deze leveranciers worden geëvalueerd en indien nodig aangepast. Een format voor deze overeenkomsten worden opgesteld door de huidige FG en met instructie ter beschikking gesteld aan de inkoopafdelingen landelijke diensten en de gerechten.	25 mei ☺
Verwerkersafspraken (overheidspartijen)	De Rechtspraak wisselt gegevens uit met, en krijgt gegevens van, diverse ketenpartijen en neemt informatiediensten af van het ministerie van BZK (P-direkt) en JenV (Leonardo). Binnen het Rijk is de regel dat overheidspartijen onderling geen verwerkersafspraken hoeven af te sluiten. De Rechtspraak maakt dergelijke afspraken wel. De komende maanden zullen deze afspraken geïnventariseerd worden en indien nodig worden aangepast. Gezien het gebruik binnen het Rijk wordt hier een lage prioriteit aan gegeven.	25 mei 😐
Privacy Impact Assessment & Privacy by design	Een PIA dient te worden uitgevoerd bij initiatie van nieuwe processen en systemen. Deze procedure is relevant voor IVO en LDCR. De procedure voor de privacy impact assessment (PIA) wordt reeds uitgevoerd door IVO. Voor de PIA wordt het Rijksmodel gehanteerd en er wordt een addendum geschreven voor de Rechtspraak. In het verlengde van de PIA wordt in de procedure voor privacy by design / default beschreven hoe privacy maatregelen worden geborgd tijdens ontwerp, ontwikkeling, implementatie en beheer. Uitrol bij IVO en LDCR.	28 april ☺
Procedures en werk instructies diensten	Het projectteam helpt de landelijke diensten bij de vertaling van de wet- en regelgeving maar operationele procedures en werkinstructies in het kader van de verwerking van persoons-gegevens. Denk hierbij bv. aan procedures voor het ontwikkelen en testen van systemen. Maart/april/mei uitrol bij IVO en LDCR.	25 mei ☺
Privacyverklaring	Aan de hand van een standaardmodel van het Ministerie van JenV wordt een op de Rechtspraak toegespitste privacyverklaring	14 mei ☺

	opgesteld. Deze privacyverklaring wordt ter vaststelling voorgelegd aan Raad en PRO	
Datalekken	Als er sprake is van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking of toegang tot persoonsgegevens dan treedt de meldprocedure datalekken in werking. Deze procedure bestaat al. De procedure voor de meldplicht datalekken wordt waar nodig aangepast aan de AVG/Richtlijn. Toetsing door FG.	Uiterlijk 25 mei ☺

Communicatie, bewustwording en educatie

Het is van belang dat communicatie, bewustwording en educatie met betrekking tot de wettelijke vereisten van de AVG en de Richtlijn en de bescherming van persoonsgegevens structureel wordt ingebed binnen de Rechtspraak. Een intern en extern communicatieplan maken daarom deel uit van de projectuitvoering. Voor educatie op het gebied van privacy is contact gelegd met de SSR.

Onderwerp	Doelstelling	Verwachting
Interne projectcommunicatie	Ten behoeve van de communicatie over de implementatie is een communicatieplan opgesteld dat gedurende het project zal worden uitgevoerd.	Tot 1 juni ☺
Interne bewustwording	Er worden maatregelen ingezet voor interne bewustwording met betrekking tot rechtmatige, behoorlijke en transparante verwerking. Er wordt deels aangesloten op het programma “jij bent de sleutel”. Dit wordt de komende maanden uitgerold en na 25 mei structureel belegd.	Doorlopend ☺
Externe communicatie	De communicatie met externe belanghebbenden over de wijze waarop de Rechtspraak invulling geeft aan de AVG en de Richtlijn is in kaart gebracht. Hier wordt in mei uitvoering aan gegeven en daarna structureel belegd. Daarnaast wordt de informatie op de privacypagina op rechtspraak.nl aangepast	25 mei ☺

Tot slot: Conclusies, aanbevelingen en actieplannen

Het voorgaande toont aan dat op veel terreinen inspanningen worden verricht om de implementatie van de privacyregels vorm te geven. Het projectteam heeft er vertrouwen in dat - dankzij de inspanningen van velen - tijdig tot het behalen van de projectdoelstellingen kan worden gekomen. Als gezegd gaat het er in de kern om dat de Rechtspraak kan aantonen in overeenstemming met de privacyregels te handelen. Veel van die inspanningen betreffen dus het inventariseren en rubriceren van reeds bestaand beleid en bestaande processen. Tijdens deze inventarisaties kunnen bevindingen in de uitvoering aan het licht komen. Bevindingen en bijbehorende acties worden in dialoog met gerechten en diensten vastgelegd in een landelijk actieplan en in (daarvan afgeleide of eigen) lokale actieplannen. Het gaat hierbij dus om bevindingen met betrekking tot de rechtmatige, behoorlijke en transparante uitvoering van beleid en werkprocessen.
In voorkomende gevallen kan het gaan om bevindingen die ook onder de huidige wet- en regelgeving als zodanig moeten worden beschouwd. In sommige gevallen is wellicht oplossing ervan op de kortst mogelijke termijn wenselijk. De datum van 25 mei 2018 is echter niet in alle gevallen van doorslaggevende betekenis. Uitvoering van de actieplannen kan ook nadien plaatsvinden, mits verantwoord.

Bij technische en arbeidsintensieve aanpassingen zal het niet altijd mogelijk zijn om vóór 25 mei 2018 de bevindingen te mitigeren. In die gevallen zal het projectteam voorzien in een advies t.b.v. de risico- en belangenafweging en het tijdspad.

De daadwerkelijke mitigatie van de bevindingen in de uitvoering is in handen van de gerechten en/of landelijke diensten. Het projectteam zal desgevraagd uiteraard hulp bieden.

Bij de tot nu toe verrichtte inventarisaties zijn de volgende aandachtspunten naar voren gekomen:

Actiepunten	**Omschrijving**
Toegang tot gegevens/autorisatie-matrices	Uit de beginselen van de AVG en de Richtlijn vloeit voort dat de toegang tot persoonsgegevens strikt beperkt moet worden tot medewerkers die noodzakelijkerwijs vanuit hun werkzaamheden toegang nodig hebben tot die persoonsgegevens. Het beeld bestaat dat gerechten en landelijke diensten werken met te ruime autorisaties in de primaire processystemen. De gerechten en diensten zullen worden gevraagd aan de hand van een op te stellen handreiking de feitelijk uitgegeven autorisaties te evalueren.
Bewaren van gegevens	Vanuit de beginselen van de AVG en de Richtlijn mogen persoonsgegevens (in dossiers en registraties) niet langer bewaard worden dan noodzakelijk voor het doel. Een eerste inventarisatie heeft uitgewezen dat de Rechtspraak achterstanden heeft als het gaat om het schonen van dossiers. Het projectteam zal met een pragmatisch advies komen.
Verstrekking van gegevens	Ingevolge de AVG mogen persoonsgegevens alleen op basis van een rechtmatigheidsgrondslag worden verstrekt aan derden. Het projectteam brengt de rechtmatigheidsgrondslagen en procedures voor verstrekking van gegevens in kaart en vraagt aan gerechten en diensten aan de hand van een handreiking de naleving van het verstrekkingsbeleid te bevorderen.

Mochten naar aanleiding van of in aanvulling op deze rapportage nog vragen leven, dan kan contact worden opgenomen met de lokale aanspreekpunten of met de projectleider implementatie AVG/Richtlijn: [redacted]@rechtspraak.nl.

Deelbesluit 10 - Datalekken
Document 349

de Rechtspraak

aan	**Deelnemers Presidenten – Raad Overleg**
van	□ voorzitter project-/werkgroep, [redacted] (bureau Rvdr)
doorkiesnummer	06-[redacted]
datum	01 mei 2018
onderwerp	Implementatie AVG en Richtlijn

Oplegmemo t.b.v. Presidenten – Raad Overleg (PRO)

Datum PRO: 14 mei 2018
Thema: Project implementatie AVG en Richtlijn
Aard agendapunt: Ter vaststelling / instemming / besluitvorming

1. Instemmen met beleidskader

Het PRO wordt gevraagd in te stemmen met de inhoud van:
- Privacy Governance Rechtspraak
- Privacybeleid Rechtspraak
- Privacyverklaring Rechtspraak en de publicatie daarvan op rechtspraak.nl

Instemming kan uiteraard ook plaatsvinden onder voorwaarde van doorvoeren wijzigingen.

2. Concrete inrichting governance

Het PRO wordt in het kader van de opzet van de governance-structuur gevraagd:
- Een lid van het gerechtsbestuur aan te wijzen als portefeuillehouder privacy
- Een medewerker van het gerecht aan te wijzen als privacy coördinator;
- Een medewerker van het gerecht aan te wijzen als coördinator informatieverzoeken;
- Hoofden van afdelingen en teams te informeren over de verantwoordelijkheden van henzelf en medewerkers in het kader van de toepassing en naleving van de AVG en de Richtlijn.

En de privacy coördinator hierover te laten terug koppelen aan het projectteam.

Nadere toelichting

De privacy coördinatoren en de coördinatoren informatieverzoeken fungeren als aanspreekpunten voor de FG. Het is van belang dat deze worden aangewezen in verband met landelijke afstemming over het ontwikkelen en uitrollen van landelijk beleid, het landelijk register van verwerking, de procedure datalekken en de procedure rechten betrokkenen.

De gerechten hebben in het kader van de implementatie AVG/Richtlijn reeds aanspreekpunten privacy gedurende het project aangewezen. Het is thans gebruikelijk dat de rol van privacy coördinator wordt uitgevoerd door een beveiligingscoördinator of een bestuurssecretaris. Als het gaat om afhandelen van verzoeken van betrokkenen betreft het meestal de bestuurssecretaris of de klachtenfunctionaris.

De gerechten zijn vrij om zelf een nadere invulling te geven aan deze rollen en de inbedding van deze rollen in de organisatie en de formatie. Dit kan ook na 25 mei. Vóór 25 mei is het in ieder geval van belang dat op centraal niveau bekend is, wie (eventueel tijdelijk) deze rollen vervullen.

de Rechtspraak

Inrichting extern toezicht (HR)
Tijdens het PRO van 14 mei zal tevens gesproken worden over de inrichting van het externe toezicht. De stukken hiervoor zijn afkomstig van de HR en de RvS. Deze stukken worden na afstemming met [redacted] apart toegestuurd naar het PRO.

Korte toelichting op de voortgang van de implementatie AVG
Tijdens het PRO van 08 maart is gemeld dat op 25 mei, kort gezegd, de volgende resultaten worden behaald:

- Governance op orde;
- Privacybeleid, privacyverklaring, procedures en richtlijnen op orde;
- Register van verwerkingen op orde;
- Actieplan op basis van bevindingen voor na 25 mei.

Het register van verwerkingen is compleet op 25 mei met dank aan inventarisatie van 155 IT applicaties door IVO, inventarisaties door landelijke diensten en inventarisaties van lokale applicaties en lijsten met persoonsgegevens door gerechten. Na instemming van het PRO met de governance en het beleid is ook dat op orde.
Wel zijn er nog een aantal bevindingen die worden opgenomen in het actieplan voor na 25 mei. Deze bevindingen zijn reeds gemeld op het PRO van 08 maart en hebben betrekking op autorisatiebeheer, uitwisseling van gegevens met externe actoren en het bewaarbeleid.

Eindrapportage
In juni zal een eindrapportage geschreven worden met nadere toelichting op het verloop van het implementatietraject en een uitgewerkt actieplan voor de toekomst welke met de gerechten en diensten gedeeld zal worden.

Deelbesluit 10 - Datalekken
Document 350

de Rechtspraak
Rechtbank Overijssel

Bijlage 4 Advies inzake zittingslijsten voor de pers versus privacy

aan [redacted] Landelijke beveiligingsambtenaar, Bureau BVA, Raad voor de rechtspraak
van [redacted], functionaris gegevensbescherming, Raad voor de rechtspraak
datum 3 maart 2017
Onderwerp Advies inzake zittingslijsten voor de pers versus privacy

Memo

Inleiding
In de Persrichtlijn 2013[1] heeft de Rechtspraak vastgelegd dat het gerecht een week voor de zitting gratis zittingslijsten ter beschikking stelt aan journalisten (zie artikel 2.2). Daarnaast is in artikel 2.3 opgenomen dat in strafzaken, voorlopige voorzieningen in bestuurszaken en in kort gedingen ook de dagvaardingen, verzoekschriften en beroepschriften onder embargo ter inzage liggen voor journalisten. Journalisten moesten dus fysiek naar het gerecht gaan om deze zittingslijsten in te kunnen zien. Om aan de wens van de journalisten tegemoet te komen deze informatie voortaan digitaal te ontvangen, is de Rechtspraak gestart met digitale verspreiding van deze informatie. Als tussenfase is deze informatie via e-mail verstuurd en vanaf dit jaar bieden alle gerechten de zittingsinformatie centraal aan via een beveiligde online bestandenpostbus. De bestandenpostbus is alleen voor geregistreerde journalisten toegankelijk met een persoonlijke inlogcode en wachtwoord.

Digitale zittingslijst in overeenstemming met de privacy?
Hoewel de geregistreerde journalisten ervoor tekenen dat zij de privacy van alle betrokkenen zullen respecteren, is het de vraag of deze digitale verspreiding wel in overeenstemming is met de huidige privacyregelgeving. Het blijkt dat er verschil tussen de gerechten bestaat over de inhoud en omvang van de zittingslijsten. Er zijn gerechten die de zittingslijsten verspreiden met als bijlage de hiervoor genoemde stukken als dagvaardingen in strafzaken. Deze stukken zijn dan over het algemeen niet geanonimiseerd. Dat betekent dat namen van slachtoffers maar ook namen van getuigen in strafzaken zichtbaar zijn. Daarnaast gaat het om personen die nog slechts verdachte zijn, maar ook bij naam en toenaam genoemd worden.

<u>Voorbeelden niet-geanonimiseerde zittingslijsten</u>
Hieronder heb ik een voorbeeld van een zittingslijst opgenomen waarbij de volledige tenlastelegging niet geanonimiseerd is bijgevoegd voor de journalisten. Het verkorte overzicht dat voor de tenlastelegging zit is wel geanonimiseerd, op de naam van de verdachte na.


strafrecht-arnhem-1feb-mk.pdf

In onderstaande zittingslijst is een verkort overzicht opgenomen met zaken die op zitting zullen verschijnen.

[1] Zie: https://www.rechtspraak.nl/Uitspraken-en-nieuws/Persinformatie/Paginas/persrichtlijnen.aspx

Behalve de naam van de verdachte staat hier en daar nog de volledige naam van de benadeelde partij.

rb-noord-nederland.pdf

Voorbeelden geanonimiseerde zittingslijsten

Hieronder zijn drie voorbeelden - in verschillende formats - van geanonimiseerde zittingslijsten opgenomen.

hof-amsterdam - perslijsten straf - wee

perslijst vb.pdf

Persrollen rechtbank Amsterdam 30 januar

Privacy-kader

Zittingslijsten bevatten persoonsgegevens, omdat de namen van partijen niet geanonimiseerd zijn. Bij verdachten wordt ook de geboorteplaats en de woonplaats vermeld. Deze gegevens zijn herleidbaar tot individuele personen. Een zittingslijst opstellen en verstrekken door middel van digitale verzending is een vorm van verwerken van persoonsgegevens als bedoeld in de Wet bescherming persoonsgegevens (Wbp). Artikel 6 Wbp schrijft voor dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Er moet ook een duidelijke doelstelling zijn omschreven voor de verwerking van deze persoonsgegevens (artikel 7). Daarnaast zijn strafrechtelijke persoonsgegevens volgens de Wbp bijzondere persoonsgegevens en die mogen in beginsel niet verwerkt worden (artikel 16).

Het doel van het opstellen en verstrekken van zittingslijsten is kort gezegd dat de gerechten daarmee de journalisten in staat willen stellen om hun werk te doen. De journalist krijgt hierdoor wekelijks informatie over komende en lopende rechtszaken. Hij kan op basis daarvan bepalen of hij de zitting al dan niet gaat bezoeken uit hoofde van zijn werk als journalist. Op zichzelf is dit een gerechtvaardigd doel, maar er dient altijd terughoudend te worden omgegaan met het verwerken van persoonsgegevens. Het vastleggen in een zittingslijst dient alleen te gebeuren als dat ook strikt noodzakelijk is. Dit in het kader van dataminimalisatie die de Wbp voorschrijft. Er dient altijd bekeken te worden of het doel niet op een andere manier bereikt kan worden, die minder ingrijpend is voor de betrokkenen (degenen van wie het gerecht de persoonsgegevens verwerkt) (*subsidiariteit*). Daarnaast dient de inbreuk op de persoonlijke levenssfeer van de betrokkenen niet onevenredig te zijn in verhouding tot het doel van de verwerking (*proportionaliteit*).

ADVIES

Meesturen stukken met zittingslijst?

Hoewel de zittingen op de zittingslijsten openbaar zijn, betekent dit niet dat alle zittingsgegevens ook digitaal aan een groep van geregistreerde journalisten moeten worden verstrekt. In verband met de bescherming van de persoonlijke levenssfeer van de betrokken partijen moet er worden bekeken of voldaan wordt aan de eisen van proportionaliteit en subsidiariteit. Door ook niet-geanonimiseerde processtukken als dagvaardingen in strafzaken, verzoekschriften en beroepschriften te verstrekken, vindt er een onevenredige inbreuk plaats op de persoonlijke levenssfeer van de slachtoffers, familieleden, getuigen e.d. Het verstrekken van hun namen is daarnaast niet noodzakelijk voor het bepalen door de journalist om al dan niet naar een zitting te gaan. Het advies is dan ook dit soort processtukken niet meer als bijlage met de zittingslijst mee te sturen. De drie voorbeelden hierboven van de verkorte zittingslijsten voldoen wel aan deze privacy-eisen. Overigens kan het meesturen van deze stukken op zich nog niet als een datalek worden gekwalificeerd. Conform de Persrichtlijn zijn de journalisten bevoegd van

deze stukken kennis te nemen en vindt dit ook plaats in een beveiligde omgeving en moet de journalist zich aan

bepaalde voorwaarden houden. Echter, wanneer een hack plaatsvindt en de zittingslijsten komen op straat te liggen, dan kan er wel sprake zijn van een datalek. De oorzaak is dan echter een beveiligingsincident. De wenselijkheid van het niet meer meesturen is nu ingegeven door de veranderde strengere privacywetgeving. Ook het privacy-bewustzijn is in de samenleving aan het toenemen. Het is dus een bestaande praktijk weer in overeenstemming brengen met de wenselijke praktijk.

Anonimiseren namen verdachten?
Dan blijft nog de vraag over in hoeverre namen van verdachten wel voluit mogen worden genoemd. Aan de ene kant worden de zittingslijsten beveiligd verstuurd aan een beperkte groep journalisten. Daardoor gaat het om een beperkte openbaarmaking en die is minder ingrijpend voor de verdachte dan wanneer de zittingslijsten voor iedereen zichtbaar op bijvoorbeeld www.rechtspraak.nl zouden worden gepubliceerd. Het weglaten van geboortedatum en woonplaats zou echter kunnen worden overwogen. Het beperkt de herleidbaarheid tot een individuele persoon in lichte mate. Daarnaast zou ook kunnen worden volstaan met het slechts vermelden van de initialen van verdachten. Iemand is dan alleen via het parketnummer herleidbaar tot een persoon. Aan de andere kant wordt de naam van de verdachte in de zittingszaal openbaar gebezigd en zal een journalist eerder de zaken van bekende verdachten uit de zittingslijst kunnen halen. Er zullen echter stemmen opgaan dat het vermelden van de naam een risico is dat de verdachte dan maar had moeten incalculeren. Daar staat tegenover dat er ook verdachten achteraf ten onrechte als zodanig zijn aangemerkt, zodat de gevolgen van openbaarmaking voor die groep nog groter kunnen zijn. Verder speelt mee dat journalisten ervoor tekenen dat zij de zittingslijsten niet mogen doorsturen en de informatie alleen voor de uitoefening van het beroep als journalist mogen gebruiken. Zij mogen geen tot een persoon herleidbare gegevens publiceren. Onder die voorwaarden is er dus wat voor te zeggen om de namen van verdachten in de zittingslijsten te laten staan.

Actiepunten
1) Stuurt de Rechtspraak deze zittingslijsten ook namens het Openbaar Ministerie? Deze vraag is belangrijk om vast te stellen wie precies verantwoordelijk is ingeval zich bijvoorbeeld een datalek voordoet. HetOM is namelijk ‘eigenaar’ van de tenlasteleggingen en zou dus ook een rol moeten spelen in de discussie over de inhoud van deze zittingslijsten. Is het OM op de hoogte en/of akkoord dat deze stukken onderdeel zijn van de zittingslijsten?
2) Het advies is om de tenlasteleggingen en andere processtukken niet meer in de zittingslijst op te nemen. Dan blijft toch nog het discussiepunt over wat te doen met de persoonsgegevens van de verdachte. Ik zou willen adviseren het OM ook bij deze discussie te betrekken.
3) Op dit moment heeft vrijwel elk gerecht zijn eigen format voor de zittingslijst. Is het niet een idee toch te proberen daar uniformering in te gaan aanbrengen? De kans op fouten wordt dan ook minder omdat iedereen dezelfde beperkte format moet invullen.