de Rechtspraak

Raad voor de rechtspraak

Privacykader Digitaal Procederen in het Civiele en Bestuursrecht (KEI)

datum 16 april 2015
auteur C.M. Aarde; B.J.A. Schellekens

Privacykader Digitaal Procederen in het Civiele en Bestuursrecht (KEI)

Dit privacykader geeft inzicht op welke wijze invulling gegeven wordt aan een zorgvuldige gegevensverwerking in het kader van digitaal procederen in het Civiele en Bestuursrecht (KEI)
Het betreft een flexibel document; Gedurende de ontwikkeling van de digitale systemen voor KEI kan dit door de ontwikkelingen nader worden bijgesteld. Neem hiervoor contact op met:
Raad voor de rechtspraak, Afdeling Strategie.

Inleiding
Het wetsvoorstel dat de kern vormt voor de digitalisering en modernisering van de Rechtspraak bestaat uit één wetsvoorstel dat twee proceswetten wijzigt: het Wetboek van Burgerlijke Rechtsvordering en de Algemene wet bestuursrecht.

Een belangrijke pijler van de modernisering is de vereenvoudiging en digitalisering van procedures in het civiele - (burgers en/of organisaties onderling) en het bestuursrecht (rechtszaken waarbij een overheidsorgaan is betrokken).

In het wetsvoorstel staan bepalingen die nodig zijn voor de digitale vernieuwde procesvoering. Deze gaan bijvoorbeeld over de verplichting om digitaal te procederen voor professionele procesdeelnemers en over het gebruik en geldigheid van de digitale handtekening. Particulieren kunnen digitaal procederen maar dit ook op papier blijven doen als zij dat willen.

Procesdeelnemers zijn partijen en hun gemachtigden en advocaten. Zij krijgen digitaal toegang tot het zaaksdossier: zij kunnen beveiligd inloggen, stukken indienen die in het digitale dossier terechtkomen en zien in welk stadium de procedure zich bevindt. De rechters of raadsheren die de zaak behandelen, zijn “eigenaar” van het dossier en houden de controle. Correspondentie tussen de gerechten en de procespartijen verloopt vanuit dit digitale zaaksdossier en is daar in te zien.

Om digitaal te kunnen procederen wordt op de website www.rechtspraak.nl een digitaal menu ontwikkeld waar de rechtzoekende op begrijpelijke wijze doorheen wordt geleid. Voor de burger die zelf procedeert wordt een ander (uitgebreider) formulier ontwikkeld, dan voor de professionele rechtsbijstandverlener die meer behoefte heeft aan een beknopt formulier. Voor mensen die hulp nodig hebben bij het invullen van het formulier, komt een informatiepunt waar medewerkers hen kunnen ondersteunen als zij praktische vragen hebben.

Dit privacykader ziet uitsluitend op het civiele en bestuursrecht aangezien dit kader geldt als Privacy Impact Assement bij het Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht)
De privacymaterie aangaande strafrecht en toezichtzaken wordt in andere documenten uiteengezet.

Persoonsgegevens
De ontsluiting van de gegevens in het digitale systeem wordt “Mijn zaak” genoemd voor partijen en “Mijn werkomgeving” voor rechtspraakmedewerkers.

In beide gevallen wordt het zogenaamde zaaksdossier ontsloten voor de partijen en betrokken rechtspraakmedewerkers. Dit zaaksdossier bevat geen andere persoonsgegevens dan dat de gerechten ook nu al in het huidige tijdsgewricht verwerken. Partijen verstrekken deze persoonsgegevens in de huidige praktijk vooral op papier. Daar waar nodig worden gegevens in het huidige digitale primaire processysteem opgenomen.

Het zaaksdossier bevat alle documentatie aangaande een zaak: de procesinleiding/het verzoekschrift dat op gestructureerde wijze via de beveiligde omgeving is ingediend; voortgangsinformatie aangaande de zaak; bewijsstukken; correspondentie met de gerechten en de uitspraak.

Het zaaksdossier bevat zowel persoonsgegevens als bijzondere persoonsgegevens. In die laatste categorie kan gedacht worden aan medische gegevens in bijvoorbeeld in WAO-zaken.

Het zaaksdossier kan naast persoonsgegevens ook gegevens bevatten die herleidbaar zijn naar bedrijven; de zogenaamde bedrijfsgegevens. Indirect zijn deze mogelijk weer herleidbaar naar natuurlijke personen zoals de bestuurders, op dat moment worden ook dit persoonsgegevens.
De Rechtspraak betracht dezelfde zorgvuldigheidseisen ten aanzien van persoonsgegevens als wanneer het om bedrijfsgegevens gaat.

Het webportaal Mijn Zaak (extern) en het webportaal Mijn Werkomgeving (intern) zijn de schil om de persoons- en zaaksgegevens aan de betrokkenen te ontsluiten. De meeste persoonsgegevens die moeten worden verstrekt, moeten ook nu in de papieren procedure worden versterkt.Het gaat om persoonsgegevens die voor het bestaande doel (een goede en zorgvuldige rechtspleging en procesvoering) worden verwerkt.
Een enkele uitzondering is gelegen in de verstrekking van extra gegevens die benodigd zijn om het digitale proces mogelijk te maken. Hierbij valt te denken aan een e-mailadres waarnaar de notificaties worden verzonden dat een nieuw processtuk beschikbaar is in het zaaksdossier. Een dergelijke notificatie bevat geen inhoudelijke zaakgegevens maar uitsluitend de melding dat er nieuwe stukken klaarstaan voor de geadresseerde in de beveiligde omgeving “mijn zaak”. Daarnaast is het burgerservicenummer noodzakelijk om de identiteit van de betrokkene vast te stellen, een uniek kenmerk aan een zaaksdossier te koppelen en tot ontsluitinging van het dossier en de voortgangsinformatie voor een betrokken natuurlijk persoon in een procedure. Omdat het burgerservicenummer een bijzonder persoonsgegeven is dat een extra wettelijke grondslag behoeft voor het gebruik wordt dit nummer in een latere paragraaf nader toegelicht.

Doeleinde en grondslag
De verwerking van persoonsgegevens door de Rechtspraak is noodzakelijk voor de zorg voor een goede en zorgvuldige rechtspleging en procesvoering. Procespartijen en hun gemachtigden moeten persoonsgegevens verstrekken aan de Rechtspraak zodat een correcte gerechtelijke procedure kan worden gevoerd bij het daartoe aangewezen gerecht.

Gerechtvaardigd belang
De verwerking van deze en andere persoonsgegevens is noodzakelijk voor de goede vervulling van de taak van de rechter en andere gerechtelijk ambtenaren zoals juridisch medewerkers en griffiemedewerkers en is daarmee gelegen in art. 8 sub f Wbp.

De doeleinden van de verwerking exart. 7 Wbp blijven net als in de huidige situatie de zorg voor een goede en zorgvuldige rechtspleging en procesvoering. Er zijn dus geen nieuwe of aanvullende doeleinden, wel wordt het transportmedium veranderd; van papier naar digitaal. Hierdoor ontstaat ook een uitbreiding van functionaliteiten voor de betrokkene. De processtukken worden namelijk opgeslagen in het digitale zaaksdossier dat rechtstreeks op beveiligde wijze kan worden ingezien door procespartijen. Wanneer een particulier er voor kiest om op papier te procederen, wordt aan de zijde van

de Rechtspraak nog altijd een digitaal zaaksdossier aangemaakt waarin de aan rechtspraakzijde gescande stukken worden opgenomen.

Alleen die gegevens die noodzakelijk zijn om het doel te bereiken worden verwerkt.

Toestemming
De Rechtspraak vraagt geen toestemming voor het verwerken van persoonsgegevens. Zij verwerkt de gegevens namelijk omdat dit noodzakelijk is voor de behartiging van haar gerechtvaardigde belang dat is gelegen in de publieke taak die voortvloeit uit de wet.

Verantwoordelijke
De verantwoordelijke is op grond van art. 1 sub d Wbp degene die het doel en de middelen van de gegevensverwerking vaststelt. Ingevolge art. 91 Wet op de rechterlijke organisatie zorgt de Raad voor de rechtspraak voor ondersteuning van de bedrijfsvoering van de gerechten in het bijzonder gericht op automatisering en bestuurlijke informatievoorziening. De Raad voor de rechtspraak is daartoe eigenaar van zijn eigen ICT-bedrijf spir-it die de ontwikkeling en het beheer van de digitale systemen van de Rechtspraak uitvoert.

Deze ontwikkeling van de systemen wordt in samenspraak met vertegenwoordigers van de gerechten ingezet.

Sinds de herziening van de gerechtelijke kaart wordt het digitale systeem voor de Rechtspraak gecentraliseerd. Er is sprake van een centraal systeem met een centrale dataopslag (in tegenstelling tot de eerdere situaties waarbij een gerecht over haar eigen databases en aangepaste datasystemen beschikte).

Ook in deze nieuwe situatie is en blijft ieder gerechtbestuur echter verantwoordelijk voor de juistheid van zijn eigen gegevens in een zaaksdossier dat bij dat betreffende gerecht aanhangig is gemaakt. De Raad voor de rechtspraak kan de verantwoordelijkheid voor de juistheid van de data niet op zich nemen, deze ligt bij de gerechtsbesturen.

Dit betekent dat er een gezamenlijke verantwoordelijkheid is voor de gegevensverwerking in de centrale digitale systemen van de Rechtspraak: te weten de Raad voor de rechtspraak en de gerechtsbesturen van de Rechtbanken en Gerechtshoven, CRvB en Cbb.

De Raad voor de rechtspraak faciliteert een zorgvuldige gegevensverwerking door onder andere de inzet van de Functionaris voor gegevensbescherming en de ontwikkeling van privacykaders. Daarnaast zorgt hij voor de uitwerking van de informatieplicht aan de betrokkene en geeft hij informatie op welke wijze de betrokkene zijn rechten kan uitoefenen door onder meer de inzet van de website www.rechtspraak.nl.

Dit sluit ook aan bij de uitleg van de art. 29-werkgroep van Europese toezichthouders op gegevensbescherming als het gaat over betrokkenheid van meerdere partijen als verantwoordelijke. Deze gezamenlijke verantwoordelijkheid is overigens niet nieuw, maar geldt ook al in de huidige situatie waarin de Rechtspraak haar gegevensverwerking in een deels analoge, deels digitale omgeving uitvoert.

Beheer van het systeem

De ontwikkeling en het beheer van de digitale systemen wordt uitgevoerd door spir-it. Dit is de eigen ICT-organisatie van de Rechtspraak.

Betrokken partijen
De interne verwerkers zijn medewerkers van de Rechtspraak:
rechters, gerechtsambtenaren van de rechtbank, raadsheren en gerechtsambtenaren van het gerechtshof, de Centrale Raad van Beroep, Cbb en de Raad voor de rechtspraak.

De externe betrokkenen zijn alle procesdeelnemers. Dit kunnen procesdeelnemers in de juridische dienstverlening zijn zoals advocaten, notarissen, rechtsbijstandverzekeraars en deurwaarders. Maar daarnaast ook de betrokken partijen: overheidsorganen, rechtspersonen en particulieren.
Beide categorieën kunnen zowel verstrekker als ontvanger zijn van de stukken in het zaaksdossier.

Verwerking van bijzondere persoonsgegevens: burgerservicenummer
Binnen de gegevenshuishouding van de overheid spelen persoonsnummers een spilfunctie: persoonsnummers dienen om persoonsgebonden gegevens eenduidig te identificeren. Om deze reden is het burgerservicenummer (BSN) geïntroduceerd voor de klantcontacten tussen burger en overheid waarbij het gebruik van een persoonsnummer nodig is ten behoeve van eenduidige identificatie en registratie van personen en voor de gegevensuitwisseling tussen overheidsorganisaties onderling. Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik maken van het BSN op grond van art. 10 Wet algemene bepalingen (Wabb). Art. 13 Wabb stelt dat degene aan wie een BSN is toegekend, dan wel diens wettelijk vertegenwoordiger, niet kan worden verplicht bij het verstrekken van persoonsgegevens aan een gebruiker een ander persoonsnummer te verstrekken dan het BSN dat aan hem, onderscheidenlijk aan degene die hij vertegenwoordigt, is toegekend.

Hieruit volgt dat de Rechtspraak voor haar publieke taak, i.e. rechtspleging, het burgerservicenummer dient te gebruiken voor de identiteitsvaststelling van de betrokkene gerelateerd aan het betrokken zaaksdossier.

Natuurlijke personen kunnen zich toegang verschaffen tot het digitale systeem van de gerechten via DigiD. Het is van belang dat de juiste persoon aan het juiste dossier wordt gekoppeld. Als een natuurlijke persoon inlogt door middel van DigiD ziet de dienstverlener (in dit geval het digitale systeem van de gerechten) het BSN van die natuurlijke persoon. Het is dan ook noodzakelijk dat het BSN van deze persoon bekend is in het digitale systeem van de gerechten, om bij het inloggen de koppeling naar het juiste dossier te kunnen maken.

Het gebruik van het BSN door de rechterlijke instanties voorkomt bovendien een vervuiling van gegevens in het digitale systeem. Zo kan het voorkomen dat een partij of haar gemachtigde haar eigen naam verkeerd invult (Janssen in plaats van Jansen), waardoor er verkeerde gegevens in het dossier zouden komen. Het BSN is een uniek identificerend nummer, waarmee overheidsinstanties behoren te werken (op grond van de Wabb). Het gebruik van het BSN voorkomt dat op basis van dergelijke verkeerde persoonsgegevens een partij geen toegang zou kunnen krijgen tot het dossier of dat de instanties werken met verkeerde gegevens.

De rechterlijke instanties digitaliseren ieder dossier, ongeacht of een partij op papier of digitaal procedeert. Om zo veel mogelijk een goed gebruik van het digitale systeem te bewerkstelligen is het

BSN van een betrokken natuurlijke persoon (ongeacht of hij op papier of digitaal procedeert) dan ook noodzakelijk. Hiermee voldoen de rechterlijke instanties ook aan hun plicht op grond van artikel 11 van de Wbp om maatregelen te treffen om de kwaliteit van gegevens te waarborgen. In de oude situatie moesten natuurlijke personen in veel gevallen een uittreksel uit de basisregistratie personen (BRP, voorheen het GBA) overleggen, omdat de rechterlijke instanties niet over de juiste gegevens (zoals het BSN) beschikten om zelf een BRP-controle te kunnen doen. Dat leidde tot administratieve lasten voor zowel natuurlijke personen als gemeenten. Doordat natuurlijke personen of namens hen hun gemachtigde, het BSN aan de rechterlijke instanties verstrekken, hoeven zij geen uittreksel meer te overleggen.

Burgerservicenummer en gemachtigden
Als een natuurlijke persoon een procedure start, geeft hij zijn naam, adresgegevens en BSN op. Een natuurlijke persoon heeft vanzelfsprekend de bevoegdheid om zijn eigen persoonsgegevens te verstrekken. Er is dan ook geen noodzaak om dat bij besluit te regelen. Indien een natuurlijke persoon met een gemachtigde procedeert en hij de procedure niet zelf start, verstrekt zijn gemachtigde het BSN van die natuurlijke persoon. Zo heeft de natuurlijke persoon met een gemachtigde ook zelf inzage in zijn digitale dossier. De natuurlijke persoon of namens hem zijn gemachtigde kan ook in een later stadium het BSN doorgeven, waarna hij toegang krijgt tot zijn digitale dossier.

Aangezien de gemachtigde geen overheidsorgaan is, kan hij geen grondslag voor de verwerking van het BSN aan de Wabb ontlenen. Artikel 24, tweede lid, van de Wbp stelt dat bij algemene maatregel van bestuur nadere regels kunnen worden gesteld over het gebruik van een wettelijk geregeld persoonsnummer (zoals het BSN). Bij het Besluit digitaal procederen wordt de grondslag gegeven aan gemachtigden om het BSN van hun cliënt die een natuurlijke persoon is en over een BSN beschikt, door te geven aan het digitale systeem van de rechterlijke instanties. Deze bevoegdheid geldt voor beroepsmatig rechtsbijstandverleners, gemachtigden en niet-professionele gemachtigden. De niet-professionele gemachtigde die op papier wil procederen kan langs die weg het BSN verstrekken van de natuurlijke persoon die hij vertegenwoordigt, mits die persoon over een BSN beschikt.

Het kan ook voorkomen dat een natuurlijke persoon geen BSN heeft, bijvoorbeeld als hij een asielzoeker is. In dat geval kan hij ook niet over DigiD beschikken en heeft hij zelf geen inzage in het digitale dossier. Het is in dat geval aan zijn gemachtigde om hem te informeren over de stukken in het dossier of het dossier desgewenst aan hem te verstrekken. Dat is hetzelfde als in de oude situatie. Voorstelbaar is ook dat een natuurlijke persoon zijn BSN niet wenst te overleggen. In dat geval kiest hij er bewust voor om zelf geen toegang te hebben tot zijn digitale dossier.
Juist vanwege deze categorie van natuurlijke personen is in het besluit voor een kan-bepaling gekozen. Het zou de toegang tot de rechter kunnen belemmeren indien een natuurlijke persoon of zijn gemachtigde in iedere procedure verplicht zou zijn om het BSN van deze persoon te verstrekken aan de Rechtspraak. Het kan degene die het BSN mag verstrekken niet belet worden om een proceshandeling te verrichten, als hij hierover op het moment van het verrichten van de proceshandeling niet beschikt. Zo kan het zijn dat hij bijvoorbeeld een beroepstermijn moet halen.

Het is evenwel noodzakelijk om in de gevallen waarin een BSN voorhanden is, dat aan de rechterlijke instanties te verstrekken. Zoals hierboven al is toegelicht, is het voor een goede werking van het digitale systeem noodzakelijk dat het BSN van bij procedures betrokken natuurlijke personen bekend is bij de rechterlijke instanties.

Het BSN wordt op zodanige wijze verwerkt dat het niet zichtbaar voor procesdeelnemers in het dossier

terecht komt. Door het gebruik van privacy enhancing technology wordt in het systeem de opgave van het BSN actief benadrukt waarna indien dit wordt opgegeven het nummer verder "onder water" in de systemen van de Rechtspraak wordt verwerkt. Het BSN wordt niet aan andere procesdeelnemers ter beschikking gesteld maar uitsluitend verwerkt ten behoeve van:

- Identificatie, verificatie en autorisatiedoeleinden op het eigen zaaksdossier;
- Technische controlemechanismen (denk aan verificatie met het BRP-online);
- Uniek kenmerk ten behoeve van optimalisering van de datakwaliteit.

De gerechtsdeurwaarder
In kantonzaken treedt de gerechtsdeurwaarder in het merendeel van de gevallen als gemachtigde op. In dat geval kan hij het BSN namens zijn cliënt verstrekken op grond van het eerste lid. Het kan ook voorkomen dat de deurwaarder niet als gemachtigde optreedt (bijvoorbeeld in vorderingszaken waar een verplichting tot procesvertegenwoordiging geldt), maar uitsluitend het oproepingsbericht betekent. De deurwaarder die in opdracht van zijn cliënt of diens gemachtigde een oproepingsbericht betekent voordat de procedure is gestart, kan eenvoudig en snel die procedure starten na betekening en de benodigde berichten indienen. Hij doet dat dan namens zijn opdrachtgever, maar treedt dus niet op als gemachtigde in de procedure (waardoor het eerste lid niet in deze situatie van toepassing is). In de oude situatie stuurde een deurwaarder in het algemeen de uitgebrachte dagvaarding naar de gemachtigde van zijn opdrachtgever, die de dagvaarding vervolgens zelf naar het gerecht stuurde. In sommige gevallen deed de deurwaarder dat namens zijn cliënt. Het is voorstelbaar dat de deurwaarder dit vaker zal doen nu dit digitaal kan. De deurwaarder betekent dan het oproepingsbericht en vervolgens dient hij de scan van het betekende oproepingsbericht (waarin de procesinleiding is opgenomen) in en start hij daarmee de procedure. De deurwaarder moet bij deze indiening ook invullen wie zijn opdrachtgever is en indien dat een burger is diens BSN kunnen doorgeven.

Hetzelfde geldt voor het BSN van de verweerder in vorderingszaken. Bij een aanzienlijk deel van de vorderingsprocedures is een deurwaarder betrokken. Een deurwaarder mag op grond van de huidige wet- en regelgeving voor het betekenen van een oproepingsbericht de persoonsgegevens van de verweerder controleren en diens BSN verwerken. Op grond van het besluit mag hij dit BSN vervolgens aan de gerechten doorgeven, opdat het digitale systeem de verweerder aan het juiste digitale dossier kan koppelen.

Toegang
Binnen de Rechtspraak geldt, dat slechts medewerkers die vanuit hun functie betrokken zijn bij de specifieke onderdelen van de rechtsgang, toegang hebben tot de persoonsgegevens. Daarbij krijgen zij slechts toegang voor zover dat noodzakelijk is voor hun functie. Hiertoe wordt een autorisatie- en rollenmodule in het digitale systeem ingebouwd.

Partijen krijgen toegang tot Mijn Zaak. De Rechtspraak draagt er zorg voor dat persoonsgegevens die in het digitale systeem worden opgenomen worden afgeschermd en beveiligd via de technische mogelijkheden die als overheidsstandaard voor beveiliging zijn aangewezen. Opdat partijen en belanghebbenden niet meer toegang wordt gegeven dan in het kader van de procedure noodzakelijk is.

Geheimhoudingsverplichtingen

De Rechtspraak creëert afzonderlijke voorzieningen voor zaken waarin een partij verzoekt om geheimhouding van of beperking van de toegang tot van een specifiek stuk, wanneer dit voortvloeit uit de aard van het stuk of wanneer het gaat om adressen die geheim moeten blijven (vergelijk artikel 8:32 en 8:29 van de Awb)

Profilering en onderzoek
In het kader van wetenschappelijk onderzoek en beleidsonderzoek kan sprake zijn van technische analyse van gegevens, bijvoorbeeld om de rechtspleging of procesvoering te verbeteren. Het kan bijvoorbeeld gaan om de kwantitatieve analyse van zaaksgegevens gerelateerd aan een bepaald zaakstype. Een dergelijk onderzoek zal altijd binnen de kaders van de Wet bescherming persoonsgegevens (en eventueel aanvullende regelgeving) worden uitgevoerd. Onderzoeksresultaten zijn niet tot personen herleidbaar.

Functionaris gegevensbescherming
Bij de Raad voor de rechtspraak is een Functionaris voor Gegevensbescherming zoals bedoeld in art. 62 Wbp voor de Rechtspraak werkzaam. De melding ex art. 27 Wbp van de verwerking van persoonsgegevens via Mijn Zaak en Mijn Werkomgeving wordt ingediend bij deze functionaris. Deze melding wordt ook gepubliceerd op www.rechtspraak.nl. Daarnaast is de Functionaris betrokken bij de uitwerking van dit privacykader.

Kwaliteit
De gebruiker voert in eerste instantie zelf zijn gegevens in en heeft voortdurend ook de mogelijkheid om deze in zijn zaaksdossier te bekijken. Zo nodig kan hij bepaalde gegevens zelf wijzigingen. Deze correctiemogelijkheid ziet uiteraard op aantoonbare feitelijke onjuistheden zoals een verschrijving. Deze correctiemogelijkheid geeft invulling aan het recht op correctie zoals bedoeld in art. 36 Wbp. Het is niet mogelijk om de zaaksinhoudelijke gegevens en gestelde feiten te corrigeren. Daarvoor is immers de gerechtelijke procedure bedoeld.
Ook aan de zijde van de Rechtspraak zijn controlemechanismen aanwezig. Zo is het mogelijk om aan de hand van de BRP (BasisRegistratie Personen) ingevoerde NAW-gegevens te controleren en waar nodig te corrigeren.

Beveiliging
De Raad voor de rechtspraak is verantwoordelijk voor de landelijke informatiebeveiliging, zoals voortvloeit uit zijn wettelijke taak binnen de bedrijfsvoering. De Raad draagt zorg voor beleid op dit terrein, houdt toezicht op de uitvoering en rapporteert hierover.

Het beveiligingsbeleid van de Rechtspraak is beschreven in haar *Handboek Integrale Veiligheid en Beveiliging*. Deze bevat ook niet-IT gerelateerde eisen, bijvoorbeeld het beveiligen van fysieke documenten. Onderdeel van het handboek zijn de normenkaders waarin de IT gerelateerde eisen opgenomen zijn die betrekking hebben op het leveren van veilige IT-diensten door de IT-uitvoeringsorganisatie. Deze normenkaders zijn door een externe auditor geactualiseerd in het kader van de invoering van deze wet, en zijn gebaseerd volgende bronnen:

- Voorschrift Informatiebeveiliging Rijksdienst (VIR), 2007;
- Voorschrift Informatiebeveiliging Rijksdienst - Gerubriceerde Informatie (VIR-GI);
- Baseline Informatiebeveiliging Rijksdienst (BIR);
- NEN-ISO/IEC 27001:2013 en 27002:2013;
- Wet bescherming persoonsgegevens (Wbp)

- 'Richtsnoeren beveiliging van persoonsgegevens' van het College bescherming persoonsgegevens (CBP);
- Beveiligingsrichtlijnen van het Nationaal Cyber Security Center;
- Norm ICT-beveiligingsassessments DigiD;
- Kaders van European Union Agency for Network and Information Security (ENISA);

Risicoanalyse en audits
Bij alle IT-projecten van de Rechtspraak wordt een zogenaamde risicoanalyse uitgevoerd. Hierin wordt het project getoetst aan geselecteerde normen uit de normenkaders voor IT-beveiliging. Daarnaast wordt periodiek en op ad-hoc basis het niveau van beveiliging van de IT-uitvoeringsorganisatie spir-it door een onafhankelijke derde partij getoetst. Dit gebeurt op initiatief van de Raad voor de rechtspraak of de uitvoeringsorganisatie zelf.

Versleuteling en toegang
De data worden enkel versleuteld via een beveiligde verbinding verzonden.

Partijen en andere betrokkenen worden ontsloten (authenticatie en identificatie) via middelen die zijn voorgeschreven door de gerechten, deze middelen ondersteunen een twee-factor authenticatie en staan onder het toezicht van de overheid. De middelen die momenteel zijn toegelaten zijn DigiD midden voor burgers, de Advocatenpas voor advocaten en eHerkenning voor rechtspersonen en overheidsorganen.

Toegangsrechten (autorisatie) worden toegekend op basis van rollen en rechtensets, afhankelijk van het soort gebruiker en zijn rol in het dossier. Het is aan een partij om te beslissen of, en zo ja, welke medewerkers geautoriseerd zijn om handelingen te verrichten of inzage te krijgen in een specifiek dossier De rechtspraak realiseert hiertoe een autorisatievoorzieningen voor procesdeelnemers.

Continuïteit
Om de voortgang van de primaire bedrijfsprocessen die direct het rechtspreken betreffen te garanderen, heeft de Rechtspraak continuïteitsplannen en standaardprocessen voor incident- en crisismanagement; Deze zijn gericht op het voorkomen van aantasting van de continuïteit van onder andere de IT-voorzieningen en op de inzet van reservefaciliteiten (al dan niet op een alternatieve locatie), wanneer voortzetting van de belangrijkste automatiseringsactiviteiten binnen de normale omstandigheden niet langer mogelijk is. Ook de back-up en het proces van een eventuele recovery van een systeem is hierin beschreven. Daarnaast is er real-time monitoring op de systemen van de Rechtspraak en worden de handelingen van gebruikers en andere gebeurtenissen vastgelegd in *onweerlegbare logging*.
De Raad voor de rechtspraak hanteert een standaardproces voor incident en crisismanagement. Dit proces voorziet in eventuele inbreuken en beveiligingsmeldingen. Er is een calamiteitenplan aanwezig. In 2014 heeft de Rechtspraak een *responsible disclosure gepubliceerd gebaseerd op* het Nationaal Cyber Security Center (NCSC). Verder zal voortdurend worden getoetst of de procedures nog voldoen of aangepast moeten worden.

Bewaring en vernietiging
De persoonsgegevens worden bewaard en vernietigd volgens de regels uit de Archiefwet. Deze zijn nader uitgewerkt in bijbehorende besluiten. Hierin staat hoe lang de persoonsgegevens moeten worden bewaard.

Transparantie
Het doel van het verwerken van de gegevens (goede en zorgvuldige rechtspleging en procesvoering) zal over het algemeen bekend zijn bij de betrokkenen, aangezien zij zelf diegene zijn die de eerste stap zetten om de gerechtelijke procedure in gang te zetten. Bij het indienen van digitale processtukken worden gebruikers gewezen op de noodzakelijke verwerking van persoonsgegevens door de Rechtspraak. De doeleinden worden ook gepubliceerd op het overzicht van gegevensverwerkingen dat door de Functionaris voor Gegevensbescherming wordt beheerd.
De website van de Rechtspraak is duidelijk herkenbaar. Daarnaast zijn de URL's van de Rechtspraak altijd herleidbaar naar de organisatie. Ondanks het feit dat het doel van de verwerking algemeen bekend mag worden verondersteld, zal op Mijn Zaak of via Rechtpraak.nl een overzicht worden geplaatst bij wie en met welk doeleinde de verwerking van persoonsgegevens plaatsvindt.
Hiermee wordt invulling gegeven aan de informatieplicht van art. 33 Wbp.