Handboek Meldplicht datalekken voor gerechten

datum	4 december 2019
versie	2.0
auteur	[redacted]
bijlage(n)	2

Inhoudsopgave

1 Inleiding

Sinds 1 januari 2016 bestaat de verplichting om datalekken binnen 72 uur na ontdekking hiervan te melden bij de toezichthouder. In bepaalde gevallen dient ook de betrokkene wiens persoonsgegevens het betreft te worden geïnformeerd. Deze meldplicht voor datalekken lag voorheen vast in de Wet bescherming persoonsgegevens (Wbp). Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing en daarmee is de Wbp komen te vervallen. De meldplicht datalekken is echter blijven bestaan. De regels ten aanzien van de meldplicht datalekken zijn op een aantal punten gewijzigd, deze worden in hoofdstuk 2 t/m 4 besproken.

De verantwoordelijkheid voor het melden van een datalek ligt binnen de Rechtspraak bij de gerechten. De Raad voor de rechtspraak (Rvdr) is verantwoordelijk voor het melden van inbreuken op beveiligingsmaatregelen bij de landelijke diensten en de Rvdr.

De AVG creëert een uitzondering voor het doen van een melding bij de AP, indien het gaat om verwerking van persoonsgegevens door gerechten in het kader van hun gerechtelijke taken. Dit betreft alle verwerkingen van persoonsgegevens die plaatsvinden in het kader van rechtszaken. Het incident moet in een dergelijk geval wel gemeld worden, maar niet aan de AP. Binnen de Rechtspraak is gekozen om deze toezichthoudende taak verschillend te beleggen, afhankelijk van de organisatie waar het om gaat. Voor de gerechten (rechtbanken, gerechtshoven en Hoge Raad) en het parket bij de Hoge Raad is dit toezicht belegd bij de procureur-generaal (PG) bij de Hoge Raad. De Afdeling bestuursrechtspraak en de Centrale Raad van Beroep en het College van Beroep voor het bedrijfsleven zijn verantwoordelijk voor de rechtmatige verwerking van persoonsgegevens die plaatsvindt in het kader van de afhandeling van (hoger) beroepen die zijn ingesteld bij hun gerecht. Ook zijn zij verantwoordelijk voor de afdoening van klachten over inbreuken op AVG-rechten. De AVG-commissie die deze gerechten hebben ingesteld adviseert over de afdoening van AVG-klachten. De AVG-commissie is samengesteld uit rechters van de drie bestuursrechtelijke colleges.

1.1 Doel Handboek

Dit handboek beschrijft kort wat een datalek is, wanneer u deze dient te melden aan de procureur-generaal bij de Hoge Raad, de bestuursrechtelijke colleges of aan de Autoriteit Persoonsgegevens, en/of betrokkenen en hoe u dit moet doen.

Datalekteam contactgegevens

Functionaris Gegevensbescherming Rechtspraak:
Email: functionarisgegevensbescherming@rechtspraak.nl
Telefoonnr: [redacted]

Plaatsvervangend Functionaris Gegevensbescherming Rechtspraak:
Email: [redacted]@rechtspraak.nl
Telefoonnr.: [redacted]

Functionaris Gegevensbescherming Hoge Raad:
Email: Functionarisgegevensbescherming@hogeraad.nl
Telefoonnr: [redacted]

Contactgegevens PG Hoge Raad:
Email: [redacted]@hogeraad.nl
Telefoonnr: [redacted]
Adres: Postbus 20303
2500 EH Den Haag

Contactgegevens bestuursrechtelijke colleges:
BVC-er CbB en CRvB

2 Wat is een datalek?

Volgens de AVG is sprake van een datalek als zich een inbreuk voordoet op de beveiligingsmaatregelen, 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 persoonsgegevens die overgedragen, bewaard of op een andere manier verwerkt zijn (zie art. 4 lid 12 AVG).

Een inbreuk op de beveiligingsmaatregelen houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet slechts sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Bij beveiligingsincidenten, waar vermoedelijk sprake is van “een inbreuk op de beveiliging“, kunt u denken aan:

- Een kwijtgeraakte USB-stick;
- De diefstal van een laptop;
- Het achterlaten van een procesdossier in de trein;
- De diefstal van een procesdossier uit de auto van een rechterlijk ambtenaar of gerechtsambtenaar;
- Brand in de postkamer;
- Onbeveiligde papiercontainer met vertrouwelijke stukken bij grof vuil;
- Het verzenden van vertrouwelijke gegevens via onbeveiligde mail;
- Een malware-besmetting.

De meldplicht geldt niet voor ieder datalek. Het is belangrijk om eerst vast te stellen of er persoonsgegevens betrokken waren bij het incident, zo niet dan is er geen meldenswaardige datalek. Ook is het belangrijk om vast te stellen wie de “verantwoordelijke” voor de verwerking van persoonsgegevens is (par. 2.2) aangezien deze verantwoordelijk is voor het doen van de melding.

Vernietiging, verlies, wijziging & ongeoorloofde verstrekking van of toegang tot persoonsgegevens
De vernietiging van persoonsgegevens houdt in dat de gegevens niet langer bestaan. Bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan en u beschikt niet over een complete en actuele reservekopie van de gegevens. In deze situatie is er ook sprake van een datalek.

> *Voorbeeld*
> In het geval van een brand in de postkamer kan er sprake zijn van vernietiging van persoonsgegevens. Dit zou het geval zijn wanneer er brieven of dossiers verbranden en er geen kopie of andere vorm van back-up is.

Verlies van persoonsgegevens betekent dat de gegevens mogelijk nog steeds bestaan, maar dat de verwerkingsverantwoordelijke niet langer controle heeft over of toegang heeft tot de gegevens of dat hij ze niet langer in zijn bezit heeft.

> *Voorbeeld*
> Voorbeelden van verlies van persoonsgegevens zijn het verlies van een tas met dossiers waarin persoonsgegevens staan, het gestolen worden van een laptop waar persoonsgegevens op staan en de versleuteling van persoonsgegevens door gijzelsoftware (“ransomware”).

Van wijziging van persoonsgegevens kan bijvoorbeeld sprake zijn indien een bestand met persoonsgegevens gecorrumpeerd raakt.

Van ongeoorloofde verstrekking of toegang kan sprake zijn indien persoonsgegevens of de toegang tot deze gegevens zijn/is verstrekt aan personen die niet gemachtigd zijn om deze gegevens te ontvangen of in te zien.

Onrechtmatige verwerking
Onder onrechtmatige verwerking valt de aantasting, onbevoegde kennisneming, wijziging, of verstrekking van persoonsgegevens. Als u redelijkerwijs niet kunt uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet u de inbreuk beschouwen als een datalek.

> *Voorbeeld 1*
> Een rechter laat zijn tas met processtukken per ongeluk in de ontvangsthal van zijn gerecht staan. Pas na enkele uren komt hij hierachter en spoedt hij zich terug om de tas op te halen. Op basis van de camerabeelden kan de beveiliging van het gerecht zien of er iemand in de tas heeft gezeten, als dat niet het geval is kan uitgesloten worden dat onrechtmatig persoonsgegevens zijn verwerkt. Is deze situatie is geen sprake van een datalek.

> *Voorbeeld 2*
> Bij een malware-besmetting moet u ervan uitgaan dat sprake kan zijn van een datalek. Bepaalde typen malware doorzoeken de besmette apparatuur op waardevolle persoonsgegevens zoals e-mailadressen, gebruikersnamen, wachtwoorden en creditcardgegevens, om de gevonden gegevens vervolgens weg te sluizen naar een server die in handen is van de aanvaller. Een dergelijke malware-besmetting stelt de getroffen persoonsgegevens bloot aan onbevoegde kennisname en andere vormen van onrechtmatige verwerking. Andere typen malware maken bestanden ontoegankelijk voor de rechtmatige eigenaar door ze te blokkeren ('ransomware') of te versleutelen ('cryptoware').

2.1 Wat zijn persoonsgegevens?

Als er geen sprake is van verwerking van persoonsgegevens, dan is de meldplicht datalekken niet van toepassing.

De AVG definieert persoonsgegevens als "*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd (…)*".

Het betreft dus gegevens die betrekking hebben op een natuurlijke persoon en de gegevens moeten concreet iets zeggen over deze persoon. Gegevens over rechtspersonen zoals ondernemingen en dergelijke zijn derhalve géén persoonsgegevens. Dit is slechts anders wanneer de organisatie vereenzelvigd kan worden met een natuurlijke persoon. Zo zegt de omzet van een eenmanszaak iets over het inkomen van de eigenaar van de eenmanszaak.

De AVG is niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn. Binnen de rechtspraak wordt echter als regel gehanteerd dat gegevens van overleden personen wél persoonsgegevens zijn. Dit met het oog op de belangen van de nabestaanden. Dat betekent dat de persoonsgegevens van overleden personen in de uitspraken op www.rechtspraak.nl geanonimiseerd worden, tenzij de familie wel op openbaarmaking prijs stelt.

De definitie van persoonsgegevens in de AVG spreekt over identificeerbare personen. Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning vastgesteld kan worden. Er kan een onderscheid worden gemaakt in direct en indirect identificerende gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.

In de AVG wordt onderscheid gemaakt tussen gewone en bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan beïnvloeden.

Voorbeelden van gewone persoonsgegevens zijn:

- Naam, adres, woonplaats;
- Telefoonnummer;
- E-mailadres;
- Processtukken betreffende een natuurlijk persoon;

- Kentekengegevens;
- IP-adressen.

Voorbeelden van bijzondere persoonsgegevens zijn gegevens over iemands:

- Ras of etnische afkomst;
- Politieke opvattingen;
- Godsdienst of levensovertuiging;
- Lidmaatschap van een vakbond;
- Genetische of biometrische gegevens met oog op unieke identificatie;
- Gezondheid (medische gegevens);
- Seksuele leven;
- Strafrechtelijk heden en verleden.

Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is gemaakt.

2.2 Wie is verantwoordelijk?

2.2.1 Verwerkingsverantwoordelijke

De verantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking. In het geval dat deze bevoegdheden in verschillende handen liggen is sprake van gezamenlijke verantwoordelijkheid.

In de meeste gegevensverwerkingen van gerechten zal het desbetreffende gerechtsbestuur de verantwoordelijke zijn en de melding moeten doen. Indien een datalek wordt ontdekt dat niet (alleen) onder de verantwoordelijkheid van het gerecht valt, dient u de andere organisatie zo snel mogelijk op de hoogte te stellen.

Oorsprong datalek bij:	Melding aan AP/PG HR/bestuursrechtelijke colleges door:	Melding aan betrokkenen door:
Gerecht	Gerecht	Gerecht
Landelijke dienst (IVO, LDCR, SSR)	Betreffende landelijke dienst	Betreffende landelijke dienst
Raad voor de rechtspraak	Raad voor de rechtspraak	Raad voor de rechtspraak
Advocaat	Advocaat	Advocaat
Ketenpartner	Ketenpartner	Ketenpartner

2.2.2 Verwerker

Indien u gegevens laat verwerken door een externe partij, is deze partij verwerker. Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen. Van verwerking door een verwerker is bijvoorbeeld sprake bij het verwerken van persoonsgegevens in de Cloud of bij externe hosting van een website waar persoonsgegevens worden verwerkt.

Als u persoonsgegevens laat verwerken door een verwerker, dan moet u ervoor zorgen dat deze voldoende waarborgen biedt ten aanzien van de naleving van de meldplicht voor datalekken. U zorgt ervoor dat de verwerker de maatregelen treft die nodig zijn zodat u aan de meldplicht voor datalekken kunt voldoen. U dient in ieder geval de volgende punten te regelen:

- Heeft u een verwerkersovereenkomst gesloten met de verwerker?
- Gaat de verwerker u daadwerkelijk informeren over alle relevante incidenten?
- Gaat de verwerker eventueel zelf meldingen doen aan de Autoriteit Persoonsgegevens?
- Ontvangt u per incident alle informatie die u nodig heeft?
- Hoe gaat de verwerker u informeren over de incidenten?
- Wordt u tijdig geïnformeerd over de incidenten?
- Wordt u op de hoogte gehouden van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die de verwerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen?
- Kunt u vaststellen dat u daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt?

3 Wanneer dient een datalek te worden gemeld aan de toezichthoudende autoriteit?

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 (art. 33 lid 1 AVG)

Met de meldplicht aan de toezichthouder is beoogd het toezicht op potentieel ernstige datalekken te ondersteunen. De toezichthouder moet door de verantwoordelijke worden geïnformeerd zodat de toezichthouder kan beoordelen of een onderzoek of het geven van aanwijzingen noodzakelijk is. De meldplicht stelt de toezichthouder onder meer in staat om te controleren of er adequaat op de inbreuk is gereageerd, of de inbreuk is beëindigd, of de genomen of aangekondigde beveiligingsmaatregelen voldoende zijn om nieuwe inbreuken te voorkomen, en of de personen die zijn getroffen door het datalek moeten worden geïnformeerd, en zo ja, of de verantwoordelijke dat heeft gedaan of nog gaat doen.

De drempel om te melden onder de AVG ligt lager dan onder de Wbp doordat “iedere inbreuk in verband met persoonsgegevens” moet worden gemeld, *tenzij* het niet waarschijnlijk is dat deze een risico inhoudt. Onder de Wbp gold tot 25 mei 2018 dat gemeld moest worden bij ‘ernstige nadelige gevolgen’ dit is een hogere drempel. Indien er na 25 mei 2018 een datalek wordt gevonden dat ontstond voor 25 mei 2018 dan gelden de Wbp criteria.

Zie ook “Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679’ van de Werkgroep gegevensbescherming 29 en het stroomschema in Bijlage A op de website van de AP:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf

3.1 Welke toezichthouder is bevoegd?

De AVG creëert de grondslag voor de Autoriteit Persoonsgegevens als externe en onafhankelijke toezichthouder (vergelijkbaar met de AFM of ACM). De AP heeft onder de AVG, naast de bevoegdheid van het houden van toezicht op datalekken een variatie aan taken en onderzoeks-, adviserende, corrigerende en boetebevoegdheden. Om de onafhankelijkheid van de rechterlijke macht bij de uitoefening van haar rechterlijke taken te waarborgen bevat de AVG een uitzondering. De bevoegdheid van de AP strekt zich niet uit over de verwerking van persoonsgegevens door gerechten in het kader van hun gerechtelijke taken. Het toezicht van de AP is voor wat betreft de gerechten dus beperkt tot de bedrijfsvoering.

> *Voorbeeld*
> Een medewerker stuurt een concept-vonnis per ongeluk naar een e-mailadres buiten de Rechtspraak. Het datalek hoort in dit geval niet gemeld te worden aan de AP omdat het gaat over een medewerker die gerechtelijke taken aan het uitvoeren is. Dit betekent echter niet dat helemaal geen melding gemaakt moet worden. Er moet melding gemaakt worden bij een andere toezichthouder. Hoe dit in zijn werk gaat wordt hieronder toegelicht.

De gerechten en het parket bij de Hoge Raad hebben er voor gekozen om het toezicht op de verwerking van persoonsgegevens in de rechtspraak toe te vertrouwen aan de door hen aangewezen functionarissen voor gegevensbescherming en de procureur-generaal bij de Hoge Raad. Indien bij de gerechten (rechtbanken, gerechtshoven en Hoge Raad) of bij het parket bij de Hoge Raad een datalek plaatsvindt dat de gerechtelijke taak betreft, dient derhalve een melding gemaakt te worden bij de PG bij de Hoge Raad.
Zie voor meer informatie over het toezicht op verwerking van persoonsgegevens door gerechten en het parket bij de Hoge Raad de *Regeling toezicht verwerking persoonsgegevens door gerechten en het parket bij de Hoge Raad*
(https://www.rechtspraak nl/Organisatie-en-contact/Organisatie/Hoge-Raad-der-Nederlanden/Reglementen/Documents/Regeling%20toezicht%20verwerking%20persoonsgegevens%20rechtspraak.pdf)

Onder verwerking van persoonsgegevens in het kader van de uitoefening van gerechtelijke taken wordt in deze regeling verstaan: alle verwerkingen van persoonsgegevens die plaatsvinden in het kader van rechtszaken.

De toezichthoudende rol van de PG betreft niet het toezicht op de verwerking van persoonsgegevens door de hoogste bestuursrechtelijke colleges. Voor deze bestuursrechtelijke colleges (Afdeling bestuursrechtspraak Raad van State, Centrale Raad van Beroep en het College van Beroep voor het bedrijfsleven) is de toezichthoudende taak neergelegd bij de leiding van het gerecht, geadviseerd door een nieuw ingestelde "AVG-commissie bestuursrechtelijke colleges". Meer informatie over de toezichthoudende taak van deze AVG-commissie vindt u in de Regeling verwerking persoonsgegevens bestuursrechtelijke colleges (pdf, 48 kB).
In deze regeling staan onder meer de werkwijze en de samenstelling van de AVG-commissie die advies uitbrengt over de afdoening van dit soort klachten. De AVG-commissie is samengesteld uit leden van de drie bestuursrechtelijke colleges.

3.2 Hoe en op welke termijn moet ik een datalek melden aan de toezichthouder (AP/PG HR)?

3.2.1 Termijn

De termijn voor het melden van het datalek begint te lopen zodra u een redelijke mate van zekerheid hebt dat een incident heeft plaatsgevonden dat onder de meldplicht datalekken valt ("de ontdekking"). Binnen **72 uur** na de ontdekking, doet u een melding bij de bevoegde toezichthouder. Indien u het incident later dan 72 uur na ontdekking aan de toezichthouder meldt, dan moet u motiveren waarom u de melding later heeft gedaan.

Mogelijk heeft u 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 doet u de melding op basis van de gegevens waarover u op dat moment beschikt. U kunt de melding naderhand nog aanvullen of intrekken nadat u verder onderzoek heeft verricht. De melding aanvullen of intrekken bij de AP gaat via hetzelfde formulier als benoemd in de volgende paragraaf. U klikt dan bij het eerste scherm op "Bestaande melding wijzigen" of "melding intrekken". Het is hiervoor van belang dat u het formulier van de eerste melding bij de hand heeft. Hierop staat een kenmerk dat bij de aanvulling vermeldt dient te worden.

3.2.2 Hoe melden

Autoriteit Persoonsgegevens
Op de site van de Autoriteit Persoonsgegevens staat een webformulier waarmee datalekken moeten worden gemeld die geen verband houden met de gerechtelijke taken:
https://datalekken.autoriteitpersoonsgegevens.nl

Als u geen gebruik kunt maken van het webformulier, dan kunt u de gevraagde gegevens per fax (FAX-NR: 070 - 88 88 501) toezenden aan de Autoriteit Persoonsgegevens. U moet daarbij zorgen dat u aan kunt tonen dat u de melding tijdig heeft gedaan.
U ontvangt per omgaande een ontvangstbevestiging. Deze ontvangstbevestiging registreert u in Classbase (zie Bijlage 1).

PG Hoge Raad
Op https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Hoge-Raad-der-Nederlanden/Documents/Formulier%20melding%20datalek.pdf is het meldformulier te vinden.
U ontvangt van de PG HR een ontvangstbevestiging met meldnummer. Ook deze melding moet u in Classbase registreren.

Bestuursrechtelijke colleges
Alle bestuursrechtelijke colleges maken gebruik van het meldformulier dat o.a. op de website van de Raad van State is gepubliceerd. Het meldformulier is opgenomen in de privacyverklaring, zie de link: https://www.raadvanstate.nl/privacyverklaring/.
Ook deze melding moet u tevens in Classbase registreren.

3.3 Moet ik het datalek melden aan betrokkenen?

Uitgangspunt van dit hoofdstuk is dat u al heeft vastgesteld dat u het betreffende datalek moet melden aan een van de toezichthouders. Daarnaast moet een datalek gemeld worden aan de betrokkenen personen wanneer het waarschijnlijk is dat het lek een hoog risico voor de betrokkenen oplevert (art. 34 AVG). Dit risico bestaat als het lek kan leiden tot fysieke, materiële of immateriële schade voor deze betrokkenen.

Wanneer het lek betrekking heeft op bijzondere persoonsgegevens, moet een dergelijk schade als waarschijnlijk worden beschouwd. Dit is dus het geval wanneer het persoonsgegevens betreft waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, of op persoonsgegevens die genetische gegevens of gegevens met betrekking tot de gezondheid of het seksleven, of strafrechtelijke veroordelingen strafbare feiten of daarmee verband houdende veiligheidsmaatregelen omvatten (overwegingen 75 en 85 bij de AVG). Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen onder meer leiden tot

stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of (identiteits)fraude.

Met de meldplicht aan de betrokkene is beoogd de betrokkene op de hoogte te stellen van wat er met diens gegevens is gebeurd en de consequenties die dat voor zijn belangen heeft. Door de kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan hij of zij zich, voor zover dat mogelijk is, daartegen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen (zoals vervanging van een wachtwoord).

De betrokkene hoeft niet op de hoogte gebracht te worden van het datalek wanneer (1) passende technische maatregelen zijn genomen en zijn toegepast (bijv. versleuteling), (2) achteraf passende maatregelen zijn genomen die zorgen dat het hoge risico zich niet meer voordoet of (3) mededeling onevenredig veel inspanning zou vergen.

Een datalek melden aan betrokkenen betekent dat u naar buiten treedt over een voorgevallen beveiligingsincident. Dit kan door middel van een persoonlijk bericht waarin de betrokkene(n) wordt medegedeeld wat is voorgevallen en welke maatregelen betrokkene zelf kan nemen.

3.3.1 Passende technische maatregelen

Indien u passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, dan kunt u de melding aan de betrokkene achterwege laten.

Voorbeeld
Er is een email door een medewerker gestuurd naar de verkeerde ontvanger. Indien de mail wordt ingetrokken voordat de ontvanger hem heeft kunnen openen dan heeft de verzender achteraf passende maatregelen genomen en dan is melden aan betrokkenen niet noodzakelijk.

Hieronder worden de twee belangrijkste technische maatregelen en de bijbehorende voorwaarden besproken, versleuteling en remote wiping.

3.3.2 Versleuteling

Het voornaamste voorbeeld van een technische beschermingsmaatregel is cryptografie, ook wel versleuteling genoemd. Deze paragraaf gaat in op het gebruik van cryptografie als technische beschermingsmaatregel om persoonsgegevens onbegrijpelijk of ontoegankelijk te maken voor onbevoegden. Andere technische beschermingsmaatregelen worden behandeld in het vervolg van dit hoofdstuk.

Cryptografische bewerkingen zijn bijvoorbeeld encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code). Kenmerkend voor encryptie is dat deze bewerking omkeerbaar is: door gebruik van de juiste sleutel kan de oorspronkelijke informatie worden verkregen

(decryptie). Encryptie wordt onder meer gebruikt om gegevens te beveiligen die zijn opgeslagen op draagbare apparatuur en op verwijderbare media zoals USB-sticks.

Als door de cryptografische bewerkingen die u heeft toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt u de melding aan de betrokkene achterwege laten. Tenzij:

- Er persoonsgegevens zijn vernietigd of aangetast (zie 3.2);
- Niet alle persoonsgegevens waren versleuteld op het moment van het datalek;
- De versleuteling niet adequaat genoeg is gezien de stand van de techniek;
- Datalek moet ook gemeld worden als de decryptiesleutels onderdeel waren van het lek.

Als deze uitzonderingen niet van toepassing zijn, dan is de mate waarin de technische beschermingsmaatregelen die u heeft genomen voldoende. Per concreet geval zult u moeten beoordelen of de geboden bescherming voldoende is om de kennisgeving aan de betrokkene achterwege te kunnen laten. Als u twijfelt over de adequaatheid van de technische beschermingsmaatregelen die u heeft getroffen, dan moet u het datalek melden aan de betrokkene.

Tenslotte moet u ook meewegen welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een ongeautoriseerd persoon er nu of in de toekomst alsnog in slaagt om kennis te nemen van de getroffen persoonsgegevens.

3.3.3 Remote wiping

Naast encryptie is er nog een andere technische beschermingsmaatregel waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname: het op afstand wissen van de gegevens die op een apparaat staan (remote wiping).

Door de gegevens te wissen worden deze ontoegankelijk voor onbevoegden, aangezien na een geslaagde remote wipe een eventuele aanvaller nog wel de beschikking heeft over het apparaat waarop de gegevens stonden, maar niet meer over de gegevens zelf. Een remote wipe heeft echter uitsluitend kans van slagen als aan een aantal randvoorwaarden wordt voldaan. De eerste randvoorwaarde is dat de remote wipe tijdig in gang wordt gezet, zodat een eventuele aanvaller nog geen kans heeft gehad om kennis te nemen van de gegevens. Verder moet op dat moment het apparaat waar het om gaat nog intact zijn en werken, zodat het in staat is om de remote wipe uit te voeren en de gegevens te wissen. Ook moet de toepassing die voor het wissen van de gegevens wordt gebruikt correct werken, zodat alle gegevens waar het om gaat daadwerkelijk worden verwijderd en geen sporen achterblijven waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

3.3.4 Melden aan betrokkene vereist onevenredig veel inspanning

Indien informeren van de betrokkene onevenredig veel inspanning vraagt kunt u volstaan met een openbare melding. Hierbij moet u rekening houden met het feit dat de informatie over het beveiligingsincident mogelijk ook gevolgen heeft voor betrokkenen wiens gegevens zijn gelekt.

3.4 Hoe en op welke termijn moet ik het datalek melden aan betrokkene?

3.4.1 Termijn

U moet het datalek zo snel mogelijk melden aan de betrokkenen. In tegenstelling tot de melding aan de toezichthouder is hiervoor geen tijdslimiet vastgesteld. De toezichthoudende autoriteit mag u verplichten een melding te doen aan betrokkene indien u dit nog niet heeft gedaan (art. 34 lid 4 AVG). Daarnaast kan de toezichthouder ook beoordelen of is voldaan aan de voorwaarden voor het afzien van een melding, waardoor een melding niet noodzakelijk is.

Na het ontdekken van het datalek mag u enige tijd nemen voor nader onderzoek zodat u de betrokkene op een behoorlijke en zorgvuldige manier kunt informeren. Wel moet u er rekening mee houden dat de betrokkene naar aanleiding van uw melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder u de betrokkene daarover informeert, hoe eerder deze in actie kan komen.

Net als bij de melding aan de toezichthouder kunt u er eventueel voor kiezen om de betrokkene in eerste instantie te informeren op basis van de informatie waarover u op dat moment beschikt. De betrokkene kan dan alvast maatregelen treffen om zich te beschermen tegen de gevolgen van het datalek. De informatie kan vervolgens op basis van nader onderzoek aangevuld worden. Een voorbeeld van een dergelijke situatie is dat u weet dat onbevoegden toegang hebben gehad tot een database met inloggegevens, maar dat u nog aan het onderzoeken bent of de onbevoegden ook andere persoonsgegevens hebben ingezien. U kunt in een dergelijk geval meteen al beginnen met het resetten van de getroffen wachtwoorden en met het informeren van de betrokkenen, waarbij u aangeeft dat betrokkenen, als zij elders dezelfde inloggegevens gebruiken, deze moeten wijzigen.

In de melding aan de toezichthouder moet u aangeven of u het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer u dat gaat doen. De termijn die u in de melding aan de toezichthouder aangeeft, moet u ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat u dit aan de toezichthouder weten door middel van een aanpassing van de melding.

3.5 Hoe melden aan betrokkenen

In de kennisgeving aan de betrokkene vermeldt u conform artikel 34 lid 2 AVG in ieder geval in duidelijke en eenvoudige taal :

- De aard van de inbreuk;
- De naam en contactgegevens van de functionaris gegevensbescherming;
- De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- De maatregelen die u de betrokkene aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.

Bij het beschrijven van de aard van de inbreuk kunt u doorgaans met een algemene omschrijving volstaan. U neemt uw contactgegevens op zodat de betrokkene u kan bereiken als hij of zij vragen heeft over het datalek. Verder geeft u aan wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken. U moet daarbij denken aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn. Het staat u vrij om meer informatie toe te voegen aan de kennisgeving, maar dit is niet verplicht.

U doet de kennisgeving aan de betrokkene op zo een manier dat een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd. Hierbij moet rekening worden gehouden met 1. de aard van de inbreuk, 2. de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, 3. de kring van betrokkenen, en 4. de kosten van tenuitvoerlegging. In veruit de meeste gevallen zult u als verantwoordelijke beschikken over de contactgegevens van de betrokkenen, en zult u in staat zijn om de betrokkenen individueel te informeren. Ingeval een betrokkene een advocaat heeft, dan geldt melding aan de advocaat als melding aan de betrokkene. Bij meer omvangrijke incidenten kunt u kiezen voor een combinatie van algemene voorlichting en het op individuele basis informeren van betrokkenen. Stem de melding aan de betrokkene ook af met uw communicatieadviseur.

> *Voorbeeld combinatie algemene voorlichting en voorlichting op individuele basis*
> U stuurt een brief naar de betrokkenen waarin u kort aangeeft wat er is gebeurd, excuses maakt, en de betrokkene erop wijst wat hij of zij zelf kan doen om de negatieve gevolgen tegen te gaan In de brief aan de betrokkenen verwijst u naar meer uitgebreide informatie op uw website. Daar licht u de aard van de inbreuk en de maatregelen die de betrokkene zelf kan treffen waar nodig nader toe. Verder verwijst u in de brief naar een centraal informatiepunt (een telefoonnummer) waar de betrokkene nadere informatie kan verkrijgen. Het belangrijkste is, dat u zo veel mogelijk betrokkenen bereikt met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel

mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt.

3.6 Vastlegging van het datalek in Classbase[1]

In de AVG is opgenomen dat een verantwoordelijke alle inbreuken in verband met persoonsgegevens (datalekken) dient te documenteren. Dit betekent dat zowel datalekken die gemeld zijn aan de toezichthouder als datalekken die niet gemeld zijn aan de toezichthouder in Classbase geregistreerd dienen te worden. Dat betekent dat onder de AVG dus ook de niet-meldenswaardige datalekken worden geregistreerd.

Het vastleggen van de datalekken heeft onder meer de volgende doelen:

- lering trekken uit het datalek en uit de wijze waarop u dit heeft afgehandeld;
- antwoord kunnen geven op vragen van betrokkenen en anderen;
- alsnog kunnen melden van het datalek aan de betrokkenen, indien u dit in eerste instantie achterwege hebt gelaten en de omstandigheden vereisen dat u dit alsnog doet.

Houdt u er verder rekening mee dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat u - waar dat aan de orde is - het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

In Classbase kunt u een melding doen door in het veld ‘aspect’ te kiezen voor de optie: ‘datalek – gemeld toezichthouder’ of ‘verlies gegevens – niet gemeld aan de toezichthouder’.
Let op: u moet alle velden invullen! Nu Classbase gebruikt wordt voor de registratie van alle beveiligingsincidenten, is het niet werkbaar om van alle velden dwingende velden te maken.

Benadrukt wordt dat het belangrijk is om de datum van ontdekking van het datalek goed te noteren. Dit is het moment waarop de 72-uurs-termijn gaat lopen om een datalek te melden bij de toezichthouder.

[1] Indien het datalek voorvalt bij een gerecht, is het betreffende gerecht verantwoordelijk voor de afhandeling van het voorgevallen datalek en registratie in Classbase. Valt het datalek voor bij één van de landelijke diensten of bij de Raad voor de rechtspraak (‘Rvdr’), dan is elk verantwoordelijk voor de afhandeling van het eigen datalek. De landelijke diensten zijn hiertoe gemachtigd door de Rvdr voor zover het datalekken betreft waarvoor de Raad verwerkersverantwoordelijke is.

4 Veel voorkomende datalekken

4.1 Anonimiseren

Tijdens het proces van anonimiseren van uitspraken zijn er gevallen waarbij gegevens niet correct zijn geanonimiseerd en persoonsgegevens zichtbaar waren op www.rechtspraak.nl. Zodra zich een beveiligingsincident heeft voorgedaan waarbij gegevens niet volgens de richtlijnen zijn geanonimiseerd, is het van belang te bekijken welke gegevens zichtbaar zijn in de gepubliceerde uitspraak en of het op basis van de onjuist geanonimiseerde gegevens mogelijk is om de betrokkene(n) te identificeren. Hoofdregel is dat anonimiseringsfouten tot de uitvoering van gerechtelijke taken horen en daardoor aan de PG HR of de bestuursrechtelijke colleges gemeld dienen te worden indien een risico voor de persoonlijke levenssfeer van het individu bestaat.

Zodra namen (van bijvoorbeeld veroordeelde, eiser, getuigen of slachtoffers) zichtbaar zijn in de uitspraak is een betrokkene direct of indirect identificeerbaar. Indien het incident echter uitsluitend om een onjuist geanonimiseerde geboortedatum gaat dan kan dat mogelijk leiden tot een andere beoordeling omtrent de identificeerbaarheid van een betrokkene.

Let wel op dat betrokkenen niet alleen op basis van de uitspraak geïdentificeerd kunnen worden, maar dat in de beoordeling tevens meegenomen dient te worden of de mogelijkheid bestaat dat onbevoegde derden in staat kunnen zijn om op grond van de onjuist geanonimiseerde informatie uit de uitspraak en reeds bestaande informatie gegevens te koppelen en zo alsnog achter de identiteit van betrokkene(n) te komen, bijvoorbeeld middels gegevens op het internet (nieuwsberichten die gepubliceerd zijn omtrent de zaak).

Zodra is vastgesteld welke gegevens zichtbaar zijn in de onjuist geanonimiseerde uitspraak, is het van belang te beoordelen of het om gegevens gaat van gevoelige, dan wel bijzondere aard. Gaat het bijvoorbeeld om een zaak betreffende een bijstandskwestie en is de naam van de betrokkene per abuis niet goed geanonimiseerd, dan zal de uitspraak veelal informatie geven over de financiële gesteldheid van deze betrokkene en kan gesteld worden dat het gaat om een zaak van gevoelige aard (namelijk financiële gegevens). Ook zodra bijvoorbeeld de naam van de veroordeelde in een strafrechtelijk vonnis per abuis niet is geanonimiseerd, kan gesteld worden dat het gaat om een zaak waarin gegevens van gevoelige aard worden verwerkt (namelijk strafrechtelijke gegevens) en kan er vanuit worden gegaan dat het datalek gemeld dient te worden. Het is echter ook goed denkbaar dat het om zaken kan gaan van minder gevoelige aard. Vandaar dat altijd beoordeeld dient te worden om wat voor soort gegevens het gaat.

4.2 Gegevensdrager zoals telefoon, usb of dossier kwijtgeraakt

Indien een gegevensdrager zoals telefoon, usb-stick of dossier is verloren, dan is het belangrijk om zo snel mogelijk over te gaan tot het nemen van technische en/of organisatorische maatregelen. Vooral als u gebruik gaat maken van remote wiping (het op afstand wissen van de gegevens die op een apparaat staan). Als door de cryptografische bewerkingen die u heeft toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt u de melding aan de betrokkene en de toezichthouder achterwege laten. Indien er persoonsgegevens zijn vernietigd of aangetast dan is melden mogelijk wel noodzakelijk. Als het gaat om persoonsgegevens uit rechtszaken, dan moet het datalek gemeld worden aan de PG HR of de bestuursrechtelijke colleges. Ook wanneer niet alle persoonsgegevens waren versleuteld op het moment van het datalek of de versleuteling niet adequaat genoeg is gezien de stand van de techniek[2].

Per concreet geval zult u moeten beoordelen of de geboden bescherming voldoende is om de kennisgeving aan de betrokkene achterwege te kunnen laten. Als u twijfelt over de adequaatheid van de technische beschermingsmaatregelen die u heeft getroffen, dan moet u het datalek melden aan de betrokkene.

U moet ook meewegen welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een onbevoegde er nu of in de toekomst alsnog in slaagt om kennis te nemen van de getroffen persoonsgegevens. Dit geldt ook bij een remote wipe waardoor kan worden aangenomen dat een eventuele aanvaller nog geen kans heeft gehad om kennis te nemen van de gegevens.

4.3 Gegevens verloren binnen de Rechtspraak

Wanneer een beveiligingsincident plaatsvindt waarbij bijvoorbeeld dossiers binnen de organisatie zijn vermist en de dossiers waarschijnlijk weer worden teruggevonden, dan is melden niet meteen noodzakelijk. Het is wel belangrijk om te monitoren of het dossier daadwerkelijk wordt teruggevonden, zo niet, dan kan er toch tot melden worden overgegaan. Dit betekent dat de melder van de vermissing benaderd moet worden en dat in de gaten moet worden gehouden of het dossier daadwerkelijk wordt teruggevonden. Het is een optie om te monitoren in hoeveel dagen een dossier gemiddeld wordt teruggevonden en deze periode als standaard wachtperiode te gebruiken. Elke vermissing moet op zichzelf worden ingeschat waarbij moet worden gelet op de context van de vermissing en het type gegevens.

[2] Het begrip “stand van de techniek” gaat in op wat gebruikelijk is in de markt en de wetenschappelijke kennis op dat moment. Als gegevens bijvoorbeeld worden versleuteld met een methode waarvan bekend is dat die methode eenvoudig gehackt kan worden, dan wordt niet voldaan aan het begrip.

4.4 Verlies gegevens door externe deskundige

Indien er een beveiligingsincident is waarbij een externe deskundige gegevens is verloren, dan is het belangrijk om de juridische verhouding tot de rechtbank te onderzoeken. Als de deskundige door de rechter is benoemd, dan is de deskundige geen 'verwerker' maar verwerkingsverantwoordelijke. Als de deskundige bijvoorbeeld het procesdossier verliest, dan moet hij dit incident zelf melden aan de AP. De deskundige dient dit incident ook altijd te melden aan het gerecht dat hem heeft benoemd. In overleg kan dan worden bepaald dat de melding aan betrokkenen door het gerecht gebeurt.

4.5 Koppeling in systeem naar verkeerde advocaat

Indien een advocaat uitsluitend notificatiemails heeft ontvangen in het systeem en dus geen inzage in de processtukken zelf heeft, hoeft er in principe geen melding gedaan te worden. De notificatiemails bevatten in een strafzaak bijvoorbeeld uitsluitend het parketnummer. Het is belangrijk om te achterhalen of er daadwerkelijk uitgesloten kan worden (d.m.v. logging) dat een ontvangende partij het dossier heeft ingezien. Het datalek valt niet onder de bedrijfsvoeringtaak, dus de melding moet aan de PG HR of de bestuursrechtelijke colleges worden gedaan. Gelet op het feit dat de foutieve ontvanger belast is met een wettelijke geheimhoudingsplicht, is de kans dat het datalek gevolgen heeft voor de persoonlijke levenssfeer verminderd, en is een melding aan betrokkene veelal niet noodzakelijk. Het incident moet dan wel in Classbase worden gemeld. Let op dat indien wel een aanzienlijk risico bestaat op schade aan de persoonlijke levenssfeer, dan zal er wel gemeld moeten worden. Je kunt dan denken aan een strafzaak van een bekende Nederlander.

4.6 Foutief verzenden van poststukken of e-mails

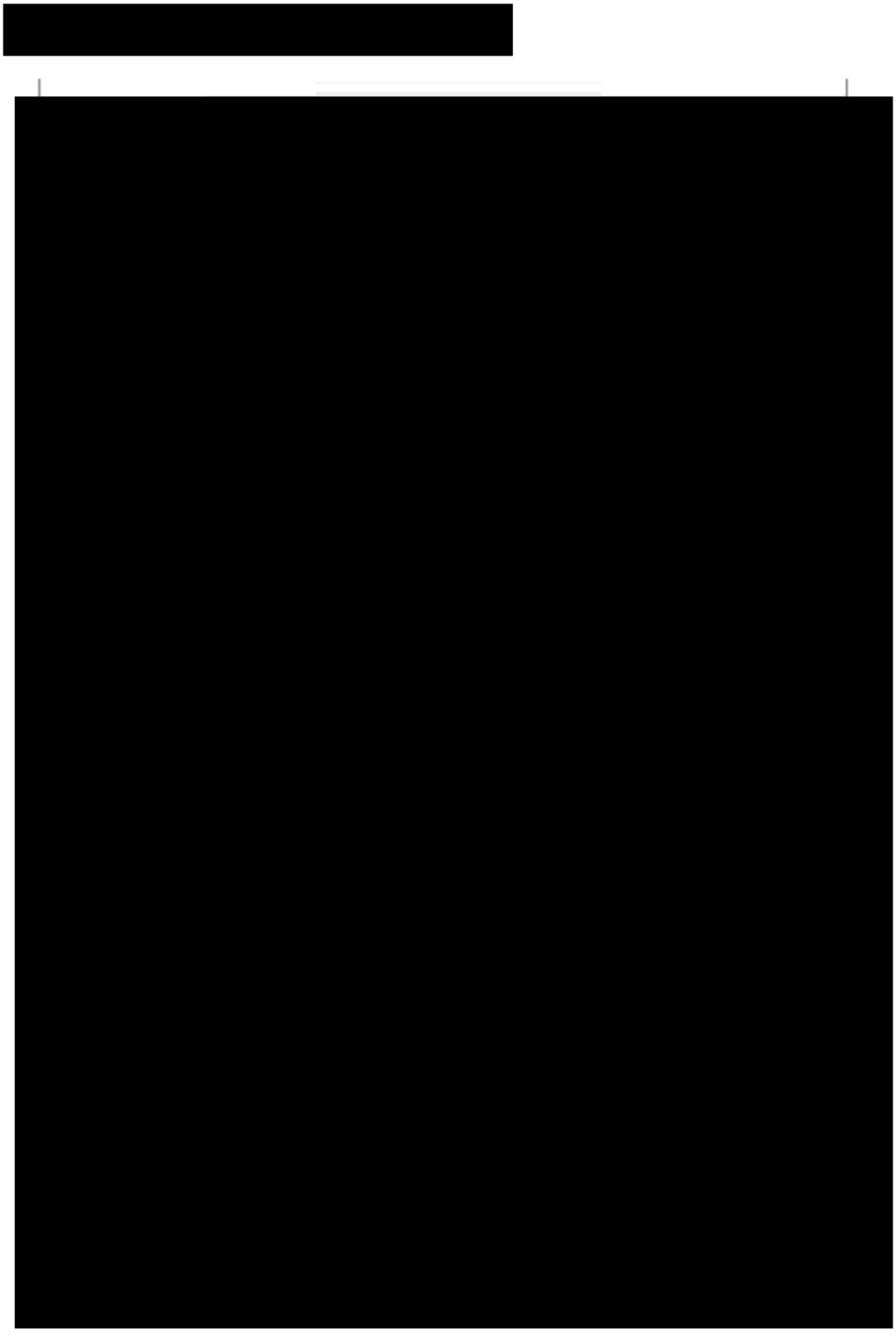
Onderzoek wie verantwoordelijk is voor het beveiligingsincident. Indien er een ketenpartner of advocaat verantwoordelijk is voor het veroorzaken van het incident, stel deze dan op de hoogte. Het gerecht is dan niet verplicht om zelf een melding te doen. Het is dan aan de advocaat of ketenpartner om de afweging te maken of ze dit incident als datalek melden aan de AP en zo ja, of ze het aan de betrokkene gaan melden.

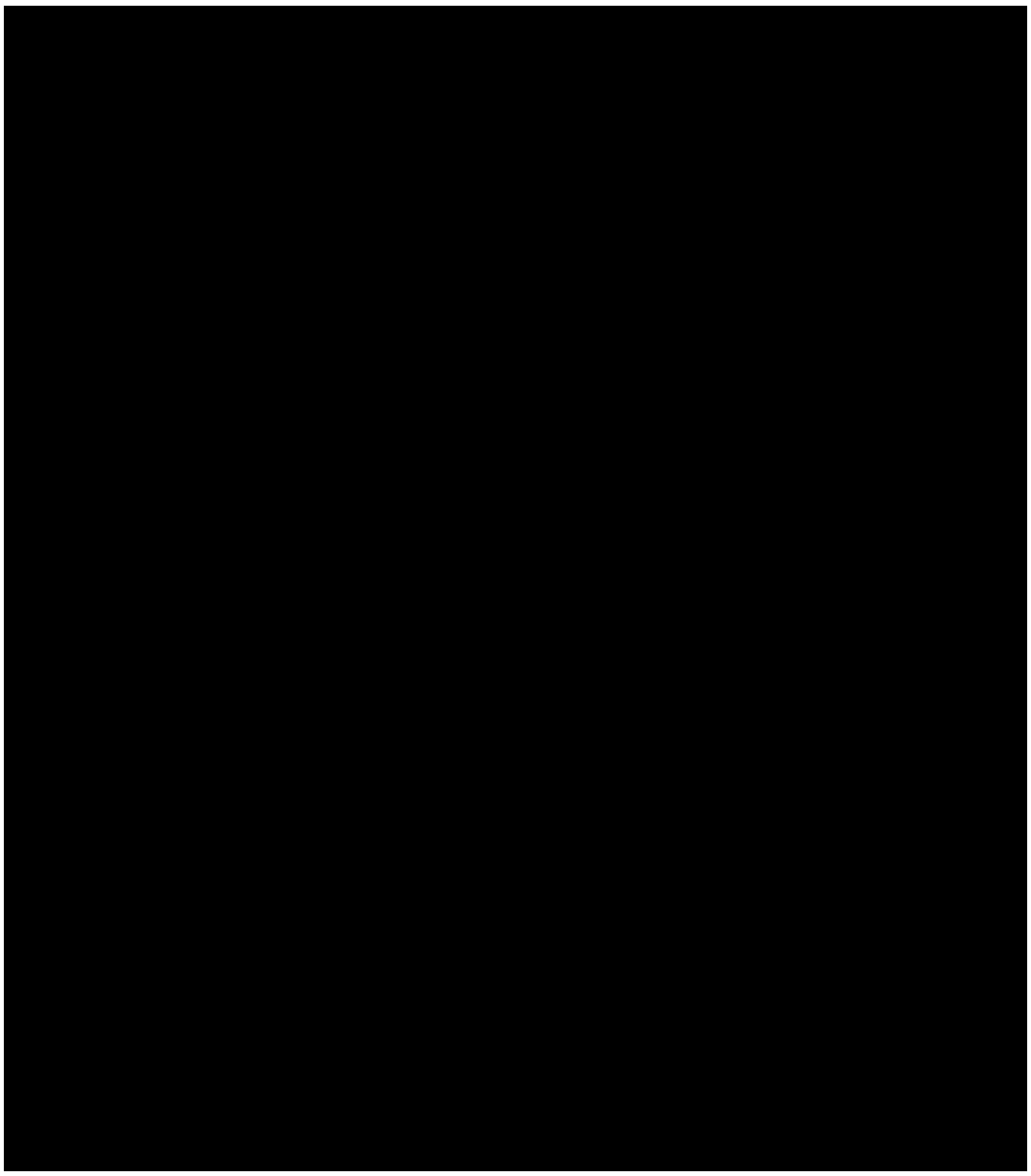
Indien de verantwoordelijkheid bij de Rechtspraak ligt en het poststuk of de email is verzonden ter uitvoering van de gerechtelijke taken is de AP niet bevoegd en moet de eventuele melding worden gedaan aan de PG HR of de bestuursrechtelijke colleges. Het is dan belangrijk om onderscheid te maken tussen verschillende soorten ontvangers. Indien de foutieve ontvanger belast is met een wettelijke geheimhoudingsplicht en heeft aangegeven de foutief ontvangen stukken te zullen retourneren, is de kans dat het datalek gevolgen heeft voor de persoonlijke levenssfeer gereduceerd, dan wel nagenoeg nihil en is een melding aan betrokkenen niet noodzakelijk. Uit het oogpunt van transparantie staat het een gerecht altijd vrij om de betrokkenen te informeren. Dat kan het geval

zijn als bijvoorbeeld een van de betrokkenen zich tot het gerecht heeft gewend om uitleg te vragen over dit incident. Dat zal naar verwachting niet vaak voorkomen.

Vraag altijd aan de ontvanger om de stukken terstond te retourneren via het gratis antwoordnummer. Als het om grote en gevoelige procesdossiers gaat, laat dan een bode van het gerecht de stukken meteen ophalen. Op die manier wordt de impact van het datalek gereduceerd.

Ook kunnen stukken per ongeluk intern binnen de Rechtspraak aan een verkeerde collega worden doorgemaild of verstuurd per post. Dat kan bijvoorbeeld een collega van het eigen gerecht zijn of een onbekende collega van een geheel ander gerecht. Als dat bijvoorbeeld stukken in een strafzaak zijn die aan een onbekende collega zijn verstuurd, dan is het advies om dit incident toch als een datalek op te vatten en te melden aan de PG HR. De collega moet dan dringend worden verzocht de stukken te vernietigen ingeval van e-mail of te retourneren in geval van poststukken.





Bijlage 2: Stroomschema datalek