AUTORITEIT
PERSOONSGEGEVENS

AP doet handreikingen om registratie datalekken te verbeteren

'Verantwoordingsplicht' onder de AVG

Sinds 25 mei 2018 is nieuwe privacywetgeving van toepassing, de Algemene verordening gegevensbescherming (AVG). De AVG legt de verantwoordelijkheid bij organisaties om aan te tonen dat ze aan de privacyregels voldoen. Eén van de verplichte maatregelen om aan de verantwoordingsplicht te voldoen is de verplichting tot het bijhouden van alle inbreuken in verband met persoonsgegevens, ofwel het bijhouden van een datalekregister. Dit staat in artikel 33, 5e lid AVG.

Het doel van deze documentatieverplichting is te stimuleren dat organisaties intern leren van eerdere inbreuken en maatregelen nemen om de kans op nieuwe inbreuken te verminderen. De documentatie biedt daarnaast handvatten om binnen de organisatie het gesprek aan te gaan in het kader van AVG-bewustzijn. Ook kan de AP als toezichthoudende autoriteit met de documentatie controleren of organisaties de meldplicht datalekken naleven.

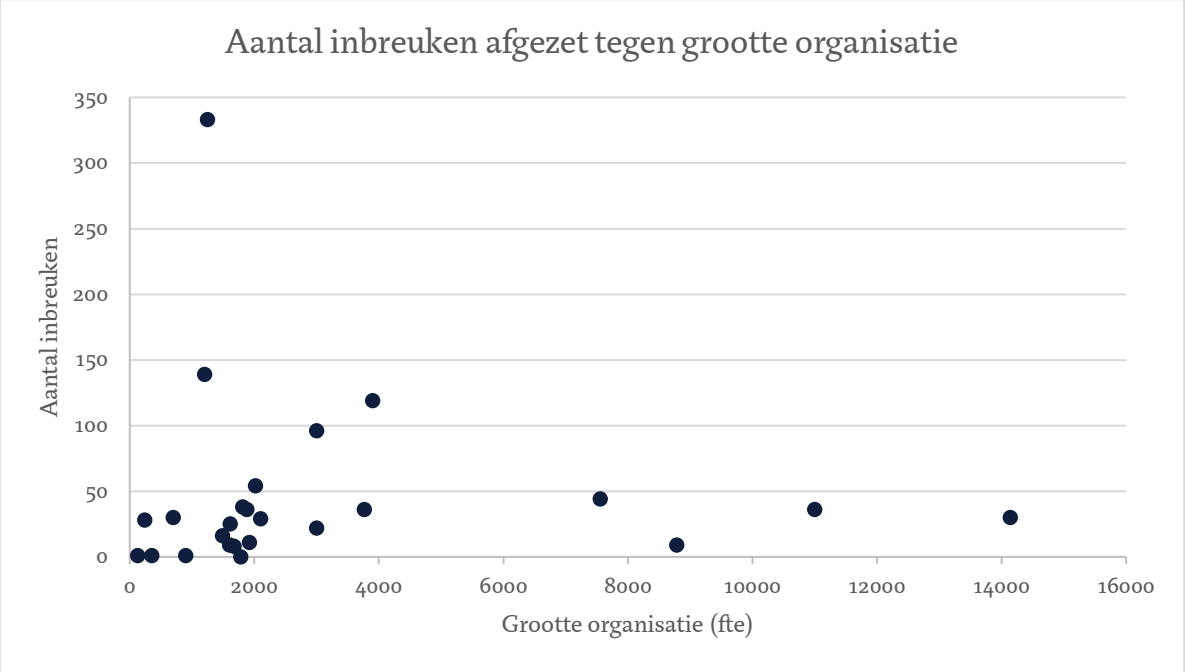
Verkennend onderzoek van de AP

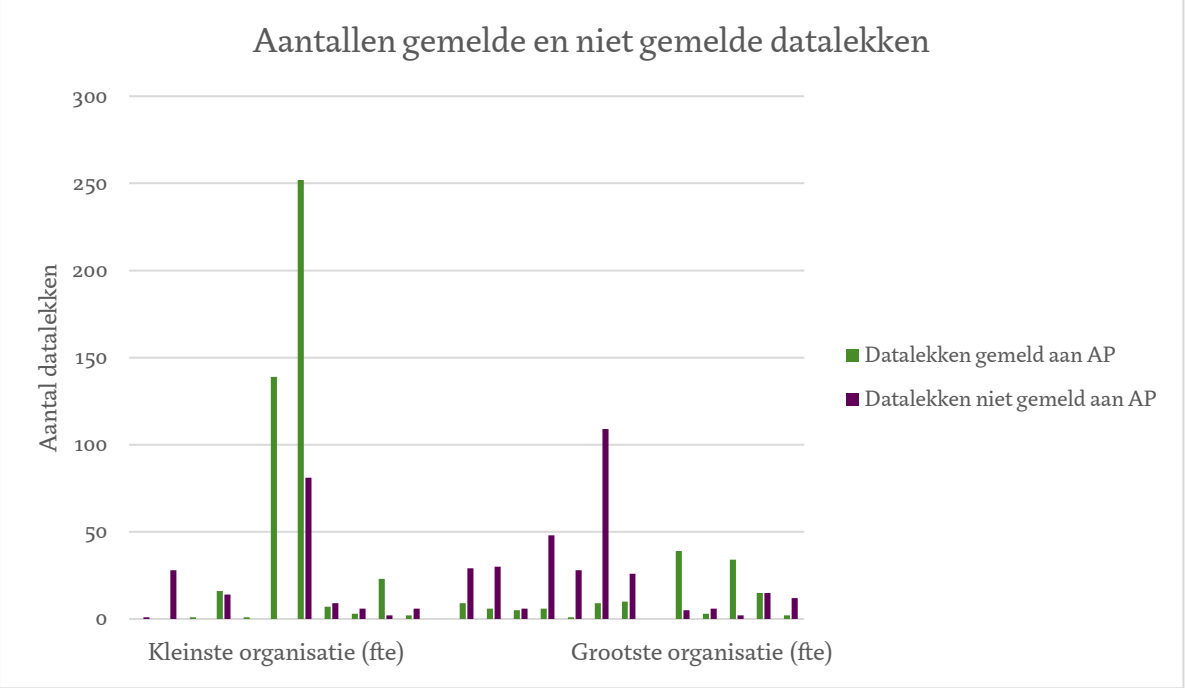
De AP heeft op 13 september 2018 26 overheidsorganisaties die veel persoonsgegevens verwerken gevraagd alle documentatie aan te leveren over de inbreuken op de beveiliging van persoonsgegevens in de periode van 25 mei tot aan 13 september 2018. Omdat de overheid een belangrijke informatiepositie en heeft eveneens een voorbeeldfunctie als het gaat om de naleving van wetgeving, is voor dit verkennend onderzoek gekozen voor de overheid. Doel van het onderzoek was om te verkennen op welke wijze organisaties invulling geven aan deze plicht. In deze rapportage deelt de AP haar beeld van de ontvangen documentatie, best en poor practices en aanbevelingen voor het bijhouden van deze registratie.

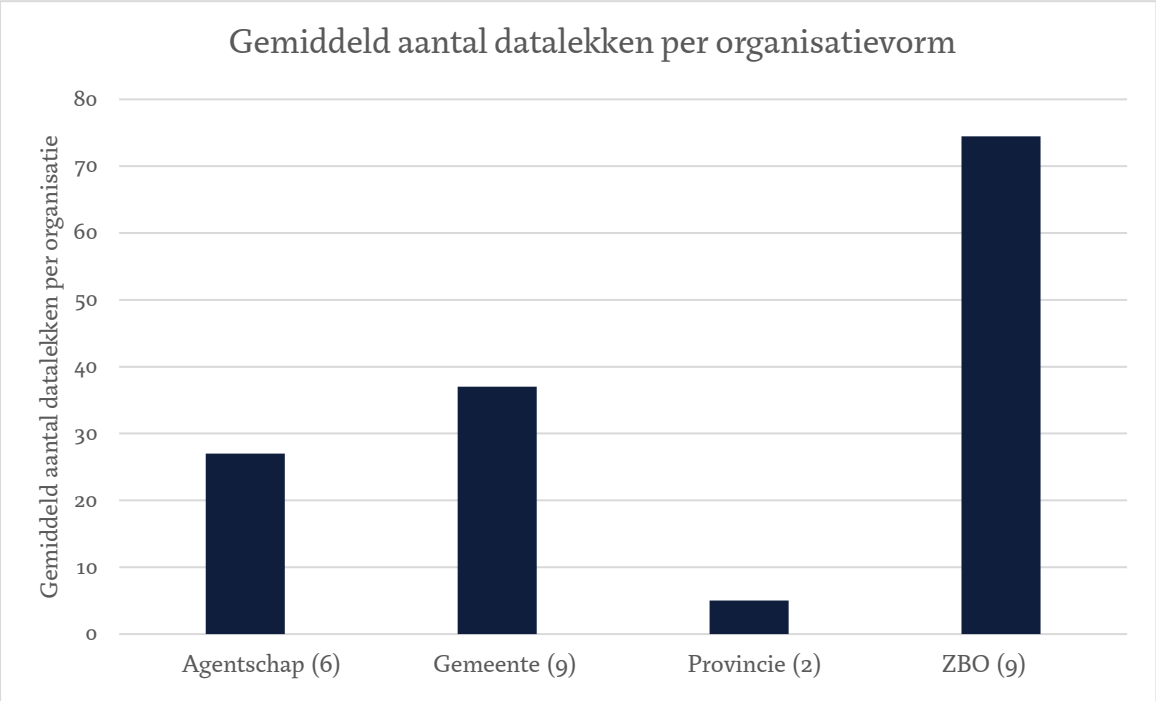
Beeld van de documentatie

De aangeleverde documentatie verschilde sterk per organisatie in opzet, inhoud en uitvoerigheid. Op basis van de vereisten uit artikel 33 AVG en de richtsnoeren datalekken hebben we alle registraties beoordeeld. Het valt de AP hoe de aantallen van de inbreuken verschillen. Van geen enkele inbreuk tot enkele honderden sinds 25 mei 2018 tot en met halverwege september 2018. De grootte van een organisatie lijkt niet veel te zeggen. Er kunnen verschillende redenen zijn waarom sommige organisaties meer inbreuken hebben gedocumenteerd dan anderen. In de volgende grafieken is af te lezen hoe de relatie is tussen het aantal gedocumenteerde inbreuken en de grote van de organisatie, de verhouding tussen de gemelde en niet gemelde datalekken, en het gemiddelde aantal datelekken per organisatievorm die wij hebben onderzocht.

De AP vat samen wat de meest voorkomende inbreuken, maatregelen en gevolgen zijn. De AP merkt hierbij wel op dat de voorbeelden die voortkomen uit de registers niet altijd voldoen aan de vereisten voor een volledige omschrijving van inbreuken, maatregelen en gevolgen.







Samenvatting meest voorkomende inbreuken

De meest voorkomende inbreuken staan hieronder in afnemende volgorde van frequentie:

1 Post, fax of 'digitale' post die niet aankomt bij de juiste persoon waarbij het om meerdere redenen mis kan gaan, zoals: onjuiste adressering, juiste adressering maar onjuiste bezorging, dubbele of verkeerde brieven die per abuis worden meegestuurd in een envelop, of kwijtgeraakte post. Met 'digitale' post bedoelen we verzending van berichten via e-mail, berichtenboxen of klantportalen. Bij deze vormen van verwerkingen gaat het ook vaak om onjuiste adressering, per abuis naar de verkeerde klant gestuurde gegevens, of verkeerd van (andere betrokkenen) meegezonden bijlages. Voorbeelden van het type persoonsgegevens die niet, of bij de verkeerde persoon terechtkomen zijn divers zoals salarisgegevens, medische gegevens, NAW gegevens, BSN etc.[1]

2 Onbedoelde/onrechtmatige inzage van persoonsgegevens intern of extern. Voorbeelden zijn de publicatie van klantgegevens op het intranet waar alle medewerkers bij kunnen, het bijvoegen van een bijlage in het verkeerde dossier zodat medewerkers onbedoeld inzage kunnen verkrijgen in (bijzondere) persoonsgegevens die niet van hun eigen klanten zijn of bijvoorbeeld medewerkers van organisaties die onbedoeld inzage krijgen in verzuimgegevens van directe collega's.

3 Het verlies van documenten of informatiedragers (zoals telefoons, laptops of tablets). Voorbeelden hiervan zijn gestolen laptops en telefoons, maar ook verloren koffers met documenten.

[1] Dit komt ook overeen met eerdere publicaties over datalekken, hier te vinden: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-ontvangt-bijna-21000-datalekken-2018

Voorbeelden van minder voorkomende inbreuken zijn: het vinden van documenten die (bijzondere) persoonsgegevens bevatten in een voor ieder toegankelijke prullenbak; printerproblemen waardoor gegevens kunnen worden ingezien door andere medewerkers of verdwijnen; hacks (4 vermoedelijke inbreuken als gevolg van hacks tegengekomen); phishing (2 vermoedelijke inbreuken als gevolg van phishing tegengekomen).

Samenvatting meest voorkomende gevolgen

De gevolgen worden vaak al meegenomen in de omschrijving van de gebeurtenis of van de feiten en omstandigheden. Sommige organisaties omschrijven bij de gevolgen ook de eventuele gevolgen die kunnen voortvloeien uit de inbreuken. Deze wijze van documenteren volgt waarschijnlijk uit het feit dat bij de beoordeling of een datalek moet worden gemeld aan de AP en/of de betrokkenen moet worden stilgestaan bij eventuele gevolgen voor de betrokkenen.[2] Het is verplicht om de daadwerkelijke gevolgen te documenteren, daarnaast mag de organisatie natuurlijk ook de eventuele gevolgen dan wel risico's opnemen.

De volgende omschrijvingen zijn voorbeelden van gevolgen die vaker voorkwamen in de registraties:

- Onbevoegde/ongeautoriseerde kennisname van persoonsgegevens;
- Blootstelling/risico op identiteitsfraude;
- Risico op stigmatisering, uitsluiting of discriminatie;
- Geen gevolgen voor de betrokkenen;
- Risico op reputatieschade;
- Gevolgen voor betrokkene(n) zijn groot vanwege expliciet verzoek om geheimhouding van de informatie betrokkenen bij de inbreuk;
- Ongunstige gevolgen voor de persoonlijke levenssfeer.

Samenvatting meest voorkomende genomen maatregelen

We constateren dat veel organisaties categorieën van maatregelen formuleren die zij herhaaldelijk registreren. We zien dat dezelfde corrigerende maatregel wordt ingezet voor dezelfde typen inbreuken.

De volgende omschrijvingen zijn voorbeelden van genomen maatregelen die vaker voorkwamen in de registraties:

- Zorgvuldiger omgaan met het versturen van documenten per post – aandacht aan besteden bij afdeling administratie;
- Meer awareness creëren voor zorgvuldiger omgaan met persoonsgegevens, wordt meegenomen in een organisatie brede awareness campagne;
- Medewerkers voorlichten over meer zorgvuldige omgang met social media;
- Extra checks/controles inrichten in het werkproces;
- Inzet van concrete maatregelen zoals verwijdering of vernietiging van de gegevens of extra beveiliging t.b.v. de data die betrokken is bij de inbreuk;

[2] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, p.10

- Postproces verbeteren;
- Informatie is door verkeerde ontvanger vernietigd;
- Het interne proces is geëvalueerd;
- De gestolen/verloren informatiedrager is vanaf een afstand gewist.

De poor en best practices

Grofweg 16 van de 26 registers bevatten – in meer of mindere mate – de in artikel 33, vijfde lid, AVG genoemde basiselementen: alle inbreuken met inbegrip van de feiten daaromtrent, de gevolgen van het lek en de genomen corrigerende maatregelen. De AP ziet ruimte voor verbetering van het aantal registraties dat aan de vereisten voldoet.

De AP ziet daarin aanleiding om meer uitleg te geven over wat een goede en slechte uitvoering van de documentatieplicht is, inclusief voorbeelden. Meer uitleg en voorlichting over de registratieplicht draagt bij aan de juiste naleving van deze verplichte documentatie en het adequaat bijhouden van deze documentatie kan helpen bij het verminderen van (de kans op) toekomstige datalekken. Tijdens onze beoordeling zijn we bepaalde aspecten in registraties tegengekomen die we graag delen zodat organisaties hiervan kunnen leren.

Poor practices

- Voorkom als organisatie een onduidelijke, (te) beperkte of onvolledige omschrijving van de (feiten van) het incident, de gevolgen en genomen corrigerende maatregelen.

Bijvoorbeeld een beperkte of onbegrijpelijk omschrijving van feiten zoals: '3-P-wet/wmo dossiers', 'toegangspas', 'verkeerd adres', 'scholingslening', en 'naamgebruik DVL'. Door het gebruik van dit soort afkortingen en (zeer) korte omschrijving van feiten wordt het niet duidelijk wat er is gebeurd.

- Voorkom als organisatie een onduidelijke, (te) beperkte of onvolledige omschrijvingen bij het omschrijven van de gevolgen.

Bijvoorbeeld: onduidelijke omschrijving van gevolgen zoals: er sprake van 'geen' risico, een 'verwaarloosbaar', 'laag', 'midden', of 'hoog' risico', zonder motivering waarom er geen risico's worden gezien of welke risico's wel worden onderkend.

- Voorkom als organisatie het niet opnemen van corrigerende maatregelen en de verwarring tussen verschillende maatregelen die wel worden opgenomen. Maak expliciet onderscheid tussen corrigerende en preventieve maatregelen.

Sommige organisaties vermelden alleen preventieve maatregelen, geen corrigerende maatregelen om bijvoorbeeld de gevolgen van het huidige incident te herstellen, al is dat onderscheid niet altijd even scherp.

Verschil is dus dat sommige organisaties bijvoorbeeld gegevens m.b.t. de inbreuk vernietigen als corrigerende maatregel. Anderen vermelden bijvoorbeeld als preventieve maatregel voor het voorkomen van toekomstige inbreuken dat zij het postproces hebben geëvalueerd. Zorg ervoor dat duidelijk onderscheid wordt gemaakt tussen de (verplichte) corrigerende maatregelen en preventieve maatregelen.

- Voorkom versnippering van onderdelen van registraties, verschil in detailniveau en wisselende kwaliteit van registratie, dit kan zorgen voor een onoverzichtelijke geheel. De kwaliteit en bruikbaarheid van het register vermindert hierdoor.

Veel organisaties hebben niet één overzicht overgelegd en registreren de informatie niet in één overzichtelijk document. Een voorbeeld hiervan is dat door een organisatie een aparte lijst werd aangeleverd met vermiste mobiele telefoons waarbij het in het totale overzicht van inbreuken niet duidelijk werd of de vermiste telefoons daarin ook waren opgenomen. Een ander voorbeeld is dat sprake is van meerdere overzichten van verschillende 'typen' inbreuken waarbij niet duidelijk wordt wat de verhouding is tussen de verschillende overzichten.

Nog een voorbeeld is dat er soms voor elke individuele inbreuk gebruik wordt gemaakt van een meldingsformulier voor registratie waarbij het inhoudelijk detailniveau enorm verschilt per ingevuld formulier. Bij het ene meldformulier wordt er door een medewerker bijvoorbeeld uitgebreid bij alle kopjes informatie ingevuld, terwijl bij het andere meldformulier de helft van de onderwerpen wordt overgeslagen en zeer beknopt wordt beschreven wat de feiten, gevolgen en genomen maatregelen zijn. Sommige organisaties hebben alle informatie van alle inbreuken in één helder overzicht waarbij het detailniveau van de beschrijving en de kwaliteit een stuk meer uniform is. Als voor een medewerker bij de registratie alle eerdere registraties van inbreuken inzichtelijk zijn, kan dit bijdragen aan de uniformiteit van de registratie.

- Zorg ervoor dat de FG betrokken wordt bij de registratie. Bij de meeste registraties werd niet duidelijk of, en zo ja in welke mate, de FG betrokken is bij de datalekregistratie. Het Europees privacytoezichthoudersverband raadt aan dat een FG bijvoorbeeld kan bijdragen aan het opzetten van een structuur voor de registratie en bij de administratie die voortvloeit uit de datalekregistratie.[3]

Best practices

- Omschrijving waarom bepaalde datalekken wel of niet gemeld zijn aan de AP en/of aan de betrokkene(n). De EDPB beveelt dit ook aan in haar richtsnoeren[4], de verwerkingsverantwoordelijke kan op deze wijze aangeven waarom bepaalde datalekken wel of niet gemeld zijn en aldus aantonen dat zij de verplichting om bepaalde datalekken te melden op de juiste wijze naleeft.
- Een uniforme registratiewijze draagt bij aan de kwaliteit van de datalekregistratie, dit kan bijvoorbeeld worden bevorderd door handleidingen, trainingen of stroomschema's voor de registratie van datalekken.

[3] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, p.32
[4] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, P.31

Slechts enkele organisaties lijken duidelijke regels en of instructies te hebben ten aanzien van de wijze van registreren. Hierdoor kan de registratie van de verschillende medewerkers per lek (enorm) verschillen. Dat maakt het leren en aanpakken van structurele fouten/zwakke plekken lastig. Een categorisering van de soorten datalekken (naar aard, gevolgen, betrokkenen) en mogelijke maatregelen zou al kunnen helpen om ook ontwikkelingen in de tijd te kunnen monitoren en op grond daarvan verbeteringen door te voeren. Daarnaast kan het helpen om de registratie overzichtelijk en inzichtelijk te maken voor alle medewerkers zodat zij het registratieoverzicht kunnen consulteren voorafgaand aan hun eigen registratie. Dit kan zorgen voor een meer uniforme registratiewijze. Andere manieren waarop een uniforme registratiewijze kan worden bevorderd is door middel van handleidingen of trainingen. De FG kan bijvoorbeeld ook bijdragen aan het opzetten van een structuur voor de registraties.[5]

Daar waar er gebruik wordt gemaakt van een uniforme registratiewijze is de registratie gemakkelijker leesbaar. De organisatie kan zo beter leren van de inbreuken die hebben plaatsgevonden en van de stappen die zijn genomen ter herstel van het lek, dan wel ter voorkoming van een lek in de toekomst.

- Zorg ervoor dat de registratie maximaal benut wordt en omschrijf zowel specifieke corrigerende maatregelen als preventieve maatregelen ter voorkoming van nieuwe datalekken. Neem deze maatregelen bijvoorbeeld mee in de plan-do-check/learn-act cyclus.

Voorbeelden van helder omschreven corrigerende en preventieve maatregelen zijn:
- Het proces van doorgeleiding is geëvalueerd. De gegevens zijn onverwijld verwijderd uit de openbare pagina's. Tevens bleek bij nader onderzoek dat slechts twee collega's die gemachtigd waren om de gegevens in te zien daadwerkelijk hadden ingezien;
- De telefoon was beveiligd met een pincode en is op afstand gewist. Tevens is de synchronisatie van de telefoon uitgezet;
- De ontvanger is verzocht om de data te vernietigen. Daarnaast hebben de verantwoordelijke managers en de postkamer samen gezeten om hier bewustwording over te creëren in het proces.

- Het registreren of, en zo ja welke, andere organisaties (bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of sub-verwerkers) betrokken zijn geweest bij een inbreuk kan bijdragen aan het lerend vermogen van de organisaties ten aanzien van wat men in de toekomst kan doen om datalekken te voorkomen. Dit kan bijvoorbeeld ook worden meegenomen wanneer er nieuwe verwerkersovereenkomsten gesloten worden met de desbetreffende verwerkers.

[5] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité, p. 32

Aanpak onderzoek

Voordat de AVG van kracht werd gold de verplichting tot het bijhouden register alléén voor datalekken die gemeld moesten worden bij de Autoriteit Persoonsgegevens (AP). Onder de AVG moeten twee soorten inbreuken worden gedocumenteerd: (1) inbreuken gemeld moeten worden bij de AP en (2) inbreuken die niet hoeven te worden gemeld bij de AP.[6] De documentatie bevat over deze inbreuken in ieder geval de volgende informatie:

- de feiten omtrent de inbreuk in verband met persoonsgegevens[7];
- de gevolgen daarvan;
- de genomen corrigerende maatregelen.

De AP heeft bij dit verkennende onderzoek de aangeleverde documentatie beoordeeld op enkele aspecten uit artikel 33 van de AVG en op de richtsnoeren van het Europese privacytoezichthoudersverband over datalekken. Daarbij heeft de AP gekeken naar:

- de omschrijving van de inbreuken;
- of de feiten voldoende duidelijk omschreven waren, inclusief de vermelding van de oorzaak van de inbreuk, het verloop van de inbreuk, en de getroffen persoonsgegevens;[8]
- of de gevolgen van de inbreuken en de genomen corrigerende maatregelen zijn opgenomen.

Naast deze vereisten beveelt het Europese privacytoezichthoudersverband aan de motivering voor de besluiten over een inbreuk vast te leggen. Dit zijn bijvoorbeeld besluiten om een inbreuk niet of juist wel te melden aan de toezichthouder[9] of over de vraag of de betrokkene(n) moeten worden geïnformeerd.[10]

De AP heeft vanwege het gebrek aan motivering in de toegezonden registraties in dit onderzoek niet kunnen nagaan of de inbreuken die zijn gemeld daadwerkelijk gemeld hadden moeten worden, of dat inbreuken gemeld hadden moeten worden die niet zijn gemeld. Ook heeft de AP niet kunnen nagaan of de inbreuken terecht of onterecht zijn gemeld aan de betrokkenen vanwege een gebrek aan motivering in de toegezonden registraties.

[6] Inbreuken dienen te worden gemeld aan de toezichthouder, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

[7] De Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité verduidelijken dat onder deze 'feiten' onder meer worden verstaan: "de oorzaken, het verloop en de getroffen persoonsgegevens" p.30-31

[8] De Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van het Comité verduidelijken dat onder deze 'feiten' onder meer worden verstaan: "de oorzaken, het verloop en de getroffen persoonsgegevens". P.30-31

[9] Zie Richtsnoeren p.27: "Met name wanneer een inbreuk niet is gemeld, moet de motivering voor dat besluit worden gedocumenteerd."

[10] Zie Richtsnoeren p.27: "Indien de verwerkingsverantwoordelijke van mening is dat aan een van de voorwaarden van artikel 34, lid 3, is voldaan, moet hij afdoend bewijs kunnen leveren dat dit het geval is."

Aanlevering van de documentatie

De AP heeft voor dit onderzoek alleen de documentatieplicht zoals neergelegd in de AVG verkend. Deze documentatieplicht geldt sinds 25 mei 2018. Het lag daarom in de rede dat de documentatie bij het verzoek in september 2018 gereed zou liggen waardoor het ook direct aangeleverd kon worden.

Op 13 september 2018 heeft de Autoriteit Persoonsgegevens 26 overheidsorganisaties aangeschreven. De AP heeft van hen allemaal een reactie ontvangen; 24 organisaties hebben hun datalekregistratie overgelegd, twee organisaties hebben aangegeven dat zij geen documentatie hebben omdat zij aangeven geen inbreuken te hebben gehad in de periode van 25 mei 2018 tot 13 september 2018.

Van 26 aangeschreven organisaties hebben echter slechts 8 de documentatie binnen de gestelde termijn aangeleverd. Drie organisaties hebben de documentatie een dag later aangeleverd. De overige 16 waren een week of meer later. De reden voor die (ver)late aanlevering van de documentatie was dat sommige organisaties voor zichzelf na moesten gaan welke documenten zij zouden moeten overleggen en in welke vorm deze konden worden aangeleverd. Daarnaast bleek dat de brief van AP pas na enige tijd op de juiste plek of bij de juiste persoon binnen de organisatie terecht kwam.

De documentatie is in de meeste gevallen digitaal en al dan niet beveiligd, aangeleverd. Een deel van de betreffende verwerkingsverantwoordelijken heeft contact opgenomen met de AP over de vorm waarin of wijze waarop, de documentatie aangeleverd moest worden. De AVG stelt geen eisen aan de wijze waarop de informatie gedocumenteerd moet worden en verwerkingsverantwoordelijken mogen dus zelf de vorm kiezen.

Afsluitend

De steekproef kent een beperkte opzet en leent zich derhalve niet voor brede conclusies . Daarom volstaan we met een beknopt samenvatting. Wel hebben we naar aanleiding van dit onderzoek een aantal praktische tips geformuleerd.

Uit het voorgaande blijkt dat alle aangeschreven verwerkingsverantwoordelijken, op twee na, documentatie met betrekking tot datalekken op verzoek van de AP hebben aangeleverd. Deze twee organisaties geven aan geen inbreuken te hebben gehad tussen 25 mei 2018 en 13 september 2018 die geregistreerd kunnen worden. Daardoor konden zij ook geen registratie aanleveren.

Dit is de eerste keer dat de AP aandacht besteedt aan de naleving van deze documentatieplicht. Zij hoopt met dit verkennend onderzoek bij te dragen aan de naleving hiervan. De AP vindt het belangrijk dat deze verantwoordingsplicht goed wordt nageleefd, een adequate registratie is namelijk niet alleen verplicht op grond van de AVG, maar kan bijdragen aan vermindering van het aantal inbreuken. De AP kan daarnaast bij het controleren van de meldplicht datalekken het register opvragen bij verwerkingsverantwoordelijken.

Alle aangeschreven organisaties krijgen deze rapportage toegestuurd, waar nodig zal de AP contact opnemen met overheidsorganisaties (en hun FG) die hun registratie kunnen verbeteren naar aanleiding van deze rapportage.

Tien tips voor een goede registratie

De beoordeling van de registraties leiden tot de volgende lijst met praktische tips voor een goede registratie:

1. Omschrijf incidenten, de gevolgen en de corrigerende maatregelen duidelijk en volledig;
2. Maak expliciet onderscheid tussen corrigerende en preventieve maatregelen. Leg corrigerende maatregelen altijd vast in het datalekregister. Het kan nuttig zijn deze maatregelen mee te nemen in de plan-do-check/learn-act cyclus;
3. Voorkom versnippering van registraties; maak één overzichtelijke registratie die voor elk organisatieonderdeel tot op hetzelfde inhoudelijke detailniveau wordt ingevuld. Overweeg bijvoorbeeld om de registratie inzichtelijk te maken voor alle medewerkers zodat zij het registratieoverzicht kunnen consulteren voordat zij zelf iets registreren;
4. Neem per incident op of de functionaris voor de gegevensbescherming (FG) betrokken is, en zo ja in welke mate. Elke overheidsorganisatie heeft verplicht een FG.
5. Neem per incident op of het datalek is gemeld bij de AP en betrokkenen en motiveer daarbij waarom dat wel of niet is gebeurd;
6. Wees transparant richting getroffen personen als er een datalek is geweest. Communiceer hier doeltreffend en tijdig over. Bewaar het bewijs van die mededeling en neem deze op in de registratie.
7. Stel een handleiding op of verzorg een training voor de medewerkers die de datalekregistratie invullen. Deze instructie kan onderdeel uitmaken van een gedocumenteerde meldingsprocedure voor de meldplicht datalekken.
8. Leg vast welke andere organisaties betrokken zijn geweest bij een inbreuk (bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of sub-verwerkers). Dit is handig als een organisatie nieuwe verwerkersovereenkomsten sluit met de desbetreffende verwerkers.
9. Overweeg datalekken in te delen naar aard, gevolgen en betrokkenen en mogelijke maatregelen;
10. Bespreek de datalekregistratie regelmatig op het juiste niveau binnen de organisatie als onderdeel van een plan-do-check/learn-act cyclus. Zo kunnen organisaties leren van fouten. De FG kan bij deze besprekingen een actieve rol vervullen.