Afhandeling van datalekken in de jeugdzorg

Goede zorg voor jeugdzorgcliënten betekent ook goede zorg voor hun persoonsgegevens

Samenvatting

De Autoriteit Persoonsgegevens (AP) heeft onderzoek gedaan naar (de afhandeling van) datalekken in de jeugdzorg. Met het onderzoek wil de AP aandacht vragen binnen de sector Jeugdzorg voor het belang van het zorgvuldig melden en registreren van datalekken. Het uitgangspunt daarbij is dat als datalekken zorgvuldig worden afgehandeld en geleerd wordt van eerdere incidenten, de bescherming van persoonsgegevens van jeugdzorgcliënten structureel kan worden verbeterd. Tegelijkertijd wil de AP de jeugdzorginstellingen tegemoetkomen met aanbevelingen, zodat zij concrete handvatten krijgen om de bescherming van persoonsgegevens binnen hun organisatie naar een hoger niveau te tillen.

Uit het onderzoek van de AP blijkt onder andere dat alle onderzochte instellingen een intern meldbeleid voor datalekken hebben opgesteld. Dit beleid wordt in de meeste gevallen ook actief onder de aandacht gebracht van de medewerkers. Ook hebben alle instellingen een intern datalekregister. Alleen is in ongeveer de helft van de gevallen dit register niet volledig. Ook maakt een op de drie van de onderzochte instellingen (nog) geen verbeterplannen om terugkerende datalekken aan te pakken. Hierdoor ontstaat het risico dat deze instellingen belangrijke extra beveiligingsmaatregelen niet (op tijd) nemen en dat er soortgelijke terugkerende datalekken ontstaan, waardoor jeugdzorgcliënten onnodig risico lopen dat hun persoonsgegevens in verkeerde handen vallen.

Aanbevelingen AP

Het is belangrijk dat jeugdzorginstellingen het bijhouden van het datalekregister niet uitsluitend zien als een administratieve verplichting, maar vooral als middel om te leren van eerdere incidenten en deze in de toekomst te voorkomen. Instellingen kunnen het datalekregister gebruiken om op eerdere fouten te reflecteren, de effectiviteit van beveiligingsmaatregelen te beoordelen en waar nodig verbeteringen door te voeren. Daarmee kan het register een belangrijke bijdrage leveren aan betere bescherming van persoonsgegevens.

Naar aanleiding van het onderzoek geeft de AP de volgende aanbevelingen:

- Leer van eerdere datalekken, maak een verbeterplan en neem dit op in de PDCA-cyclus

Grijp elk datalek aan om uw processen te verbeteren. Analyseer zorgvuldig wat er misging, achterhaal de oorzaken, en implementeer concrete maatregelen om herhaling te voorkomen. Leg deze maatregelen ook vast in het datalekregister, zodat u de effectiviteit hiervan periodiek kunt evalueren.

Maak deze evaluatie een onderdeel van de Plan-Do-Check-Act (PDCA-)cyclus. Indien uw organisatie al een interne werkwijze heeft die het afhandelen van incidenten en calamiteiten regelt, dan kunt u de afhandeling van datalekken aan laten sluiten bij het ontwikkelde algemene proces of methode voor verbetering na een incident. Dit stelt u in staat om niet alleen incidenten af te handelen, maar ook structureel uw beveiligingsstrategie en risicomanagement te versterken op de lange termijn.

Voorbeeld van PDCA-cyclus datalekken
Als bijlage bij dit rapport heeft de AP een voorbeeld toegevoegd van een stappenplan dat periodiek kan worden uitgevoerd als onderdeel van de PDCA-cyclus. Dit stappenplan kunt u gebruiken om bij te houden of (bepaalde typen) datalekken toenemen, wat daarvan de mogelijke oorzaak is, of eerdere maatregelen hebben gewerkt om het aantal datalekken te verminderen en of er aanvullende maatregelen nodig zijn. Zo kunt u de beveiliging van persoonsgegevens voortdurend evalueren en verbeteren.

- Betrek altijd de FG bij de afhandeling van datalekken

Zorg ervoor dat de functionaris gegevensbescherming (FG) altijd vanaf het begin nauw betrokken is bij de afhandeling van datalekken. De FG speelt een cruciale rol in het bewaken van de naleving van privacyregels en heeft een adviserende en controlerende functie.

Betrek daarom de FG, zodat deze advies kan geven, en laat het bestuur als eindverantwoordelijke vervolgens de beslissing nemen of een datalek gemeld moet worden aan de AP en aan de slachtoffers van het datalek (de mensen van wie persoonsgegevens zijn gelekt).

- Zorg dat u kunt aantonen dat datalekken adequaat zijn afgehandeld

Zorg ervoor dat u duidelijk in het datalekregister vastlegt: (1) wat er is gebeurd; (2) wat de gevolgen zijn voor de slachtoffers; en (3) welke maatregelen u heeft genomen na het datalek. Daarmee is er transparantie over de stappen die zijn gezet. Dit zorgt ervoor dat zowel interne als externe belanghebbenden kunnen zien of een datalek correct is beëindigd en of er verdere risico's zijn. Benoem in ieder geval: de oorzaak van het datalek, wat er zich heeft afgespeeld, welke groep(en) personen is of zijn getroffen en om wat voor soort persoonsgegevens het gaat. Zo kunt u achteraf nagaan of een goede risico-inschatting is gemaakt, en of de slachtoffers terecht wel of niet zijn geïnformeerd.

Voorbeeld van datalekregister

Om organisaties op weg te helpen met het goed bijhouden van een datalekregister, heeft de AP een voorbeeld van een datalekregister gemaakt. Dit voorbeeld is te downloaden via de website van de AP. Alle organisaties kunnen dit voorbeeld gebruiken, ook organisaties buiten de sector Jeugdzorg. Zie: https://autoriteitpersoonsgegevens.nl/documenten/voorbeeld-datalekregister

- Zorg ervoor dat medewerkers weten wat een datalek is en hoe ze moeten handelen

Goed geïnformeerde medewerkers kunnen beter reageren op incidenten. Besteed daarom aandacht aan het thema datalekken bij de 'onboarding' van nieuwe medewerkers, bespreek/evalueer datalekken binnen het team waar ze plaatsvinden en organiseer regelmatig (verplichte) trainingen, workshops en awareness-campagnes.

1. Inleiding

1.1 Aanleiding voor het onderzoek

In 2019 en 2020 zijn er enkele grote datalekken geweest binnen de sector Jeugdzorg in Nederland. Deze datalekken hebben geleid tot Kamervragen[1] en een onderzoek van de Inspectie Gezondheidszorg en Jeugd (IGJ)[2]. De belangrijkste conclusie van dit onderzoek was dat er in de jeugdzorg onvoldoende kennis is van ICT en informatiebeveiliging. En daardoor ook niet genoeg zicht op de risico's. Ook stelde de IGJ vast dat de sector niet genoeg geld heeft. De afgelopen jaren komt de jeugdzorg dan ook veel in het nieuws vanwege financiële problemen. Meer dan 40 procent van de jeugdzorginstellingen maakte verlies over 2022.[3] Daarnaast stelde het Centraal Bureau voor de Statistiek (CBS) vast dat in 2022 50 procent van de werknemers in de jeugdzorg een '(veel) te hoge werkdruk' ervaarde.[4] Deze omstandigheden dragen bij aan het risico op datalekken bij jeugdzorginstellingen.

Voor effectieve jeugdzorg is het belangrijk dat jongeren die jeugdzorg ontvangen (hierna: jeugdzorgcliënten) erop kunnen vertrouwen dat jeugdzorginstellingen zorgvuldig omgaan met (gevoelige) persoonsgegevens die zij aan de instellingen hebben verstrekt. En dat jeugdhulpverleners hun wettelijke geheimhoudingsplicht niet doorbreken. Datalekken in de jeugdzorg kunnen dit vertrouwen beschadigen. Dit kan ertoe leiden dat jeugdzorgcliënten terughoudend worden om gevoelige gegevens over hun privésituatie te delen met jeugdzorginstellingen. Dit belemmert de uitvoering van de jeugdzorg. Daarnaast kunnen datalekken in de jeugdzorg leiden tot aanzienlijke emotionele schade voor de getroffenen. In deze sector worden immers veel gevoelige persoonsgegevens verwerkt van kwetsbare minderjarigen.

1.2 Doel van het onderzoek

De Autoriteit Persoonsgegevens (AP) heeft besloten verkennend onderzoek te doen naar (de afhandeling van) datalekken binnen de sector Jeugdzorg. Het onderzoek was erop gericht om meer inzicht te krijgen in hoe 'AVG-volwassen' deze sector is voor wat betreft de omgang met datalekken. En op basis van de tijdens het onderzoek verkregen inzichten aanbevelingen te doen, en voorbeelden mee te geven. De AP wil hiermee stimuleren dat jeugdzorginstellingen persoonsgegevens van jeugdzorgcliënten goed beschermen. En dat zij datalekken melden aan de AP en aan de slachtoffers van het datalek (de mensen van wie persoonsgegevens zijn gelekt) wanneer dat nodig is. Het informeren van slachtoffers is belangrijk, omdat dit hen in staat stelt om zich te wapenen tegen de negatieve gevolgen van het datalek. Transparantie over datalekken is daarnaast belangrijk voor het vertrouwen van jeugdzorgcliënten in de zorgvuldige omgang met hun persoonsgegevens.

1.3 Methode van het onderzoek

Het onderzoek is uitgevoerd door informatie en documentatie te analyseren die bij vijftien geselecteerde jeugdzorginstellingen is opgevraagd, waaronder:

- het datalekregister;
- het interne meldbeleid voor beveiligingsincidenten;
- informatie over algemene technische of organisatorische maatregelen die de instelling neemt om het risico op datalekken te beperken;
- informatie over maatregelen die de instelling neemt om ervoor te zorgen dat medewerkers weten hoe zij zorgvuldig omgaan met datalekken, waaronder hoe zij beveiligingsincidenten intern moeten melden.

[1] https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2019A01711
[2] https://www.igj.nl/publicaties/publicaties/2020/06/18/extra-aandacht-nodig-voor-ict-in-de-jeugdzorg
[3] https://www.jeugdzorgnederland.nl/actueel/zorgbarometer-seinen-voor-jeugdzorg-op-rood/
[4] https://www.cbs.nl/nl-nl/nieuws/2022/46/helft-zorgwerknemers-vindt-werkdruk-te-hoog

Selectieprocedure

De aangeschreven vijftien jeugdzorginstellingen zijn geselecteerd op basis van omvang[5] en het aantal datalekmeldingen dat zij vanaf 1 januari 2020 hebben gedaan bij de AP. Daarbij heeft de AP vooral instellingen geselecteerd die, gezien hun omvang, relatief weinig datalekmeldingen hebben gedaan. Instellingen waarbij de AP veel aandachtspunten constateerde, zijn uitgenodigd voor een interview. Dit gebeurde in drie gevallen. De AP heeft met deze instellingen afspraken gemaakt om een aantal zaken te verbeteren.

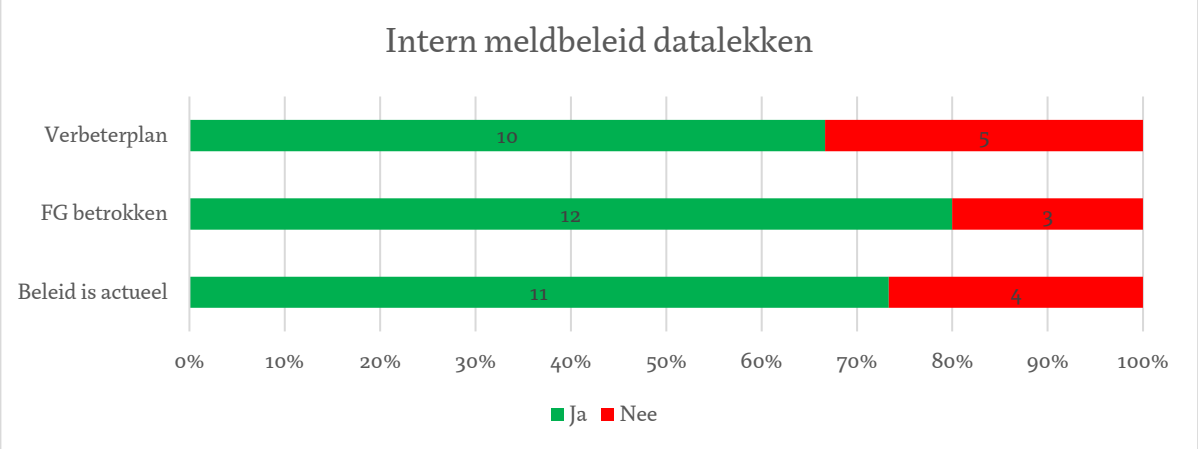
2. Intern meldbeleid voor datalekken

2.1 Belang van intern meldbeleid

Het is belangrijk voor organisaties om een gedocumenteerde meldingsprocedure te hebben voor datalekken, die de organisatie volgt zodra een datalek wordt geconstateerd. Daarin kan ook worden vastgelegd hoe de organisatie het datalek moet inperken, beheren en herstellen, het risico moet beoordelen en het datalek moet melden. Zo waarborgt de organisatie dat telkens de juiste stappen worden genomen bij een datalek. Jeugdzorginstellingen hebben mogelijk al een interne werkwijze voor het afhandelen van (cyber-)incidenten[6] en calamiteiten. Het interne meldbeleid voor datalekken kan in deze gevallen aansluiten bij het bestaande proces. Om het meldbeleid goed te kunnen uitvoeren, is het daarnaast belangrijk dat werknemers op de hoogte zijn gebracht van deze procedures en dat zij weten hoe zij op datalekken moeten reageren zodat ze goede en privacyvriendelijke zorg kunnen bieden aan hun clienten.[7]

2.2 Beoordeling intern meldbeleid

De AP heeft vijftien jeugdzorginstellingen gevraagd om hun intern beleid voor het registreren en melden van datalekken. De bevindingen staan in deze tabel:



Bij de meeste instellingen (tien van de vijftien) is het implementeren van verbetermaatregelen na een datalek, of het onderzoeken daarvan, al een vast onderdeel van het datalekbeleid. Bij vijf van de vijftien instellingen is dit nog niet zo. Deze organisaties trekken nog onvoldoende lering uit eerdere datalekken. Hierdoor neemt het risico toe dat bepaalde soorten datalekken opnieuw plaatsvinden.

[5] Gemeten in aantal medewerkers en/of het aantal jeugdzorgcliënten.
[6] Zie: NEN 7510-2:2017 hoofdstuk 16 en 17 inclusief bijlage C. Zie ook: Handreiking informatiebeveiliging Jeugdinstellingen Aanbevelingen voor veiligere IT in de jeugdzorg, Kenmerk: HB/dd/20-1875a, Hoofdstuk 7 "Incident response".
[7] Zie ook: Richtsnoeren 9/2022 betreffende melding van inbreuken in verband met persoonsgegevens uit hoofde van de AVG, Versie 2.0 (hierna: Richtsnoeren 9/2022), p. 31.

Aanbeveling: Leer van eerdere datalekken en evalueer maatregelen
Het is belangrijk om zoveel mogelijk lering te trekken uit eerdere incidenten, en maatregelen te nemen om het risico op nieuwe datalekken te verkleinen. De AP adviseert om dit op te nemen in de Plan-Do-Check-Act (PCDA)-cyclus, en minstens twee keer per jaar te rapporteren aan het bestuur over de datalekken in de afgelopen periode. Het is van belang dat het bestuur hier regelmatig aandacht aan besteedt, want op die manier wordt privacy een onderdeel van de organisatiecultuur. Indien uw organisatie al een interne werkwijze heeft die het afhandelen van incidenten en calamiteiten regelt, dan kunt de afhandeling van datalekken daarbij aan laten sluiten. Zo kunt u bijhouden of (bepaalde typen) datalekken toenemen, wat daarvan de mogelijke reden is, of eerdere maatregelen hebben gewerkt om het aantal datalekken te verminderen en of er aanvullende maatregelen nodig zijn. U kunt dit bijvoorbeeld beleggen bij de functionaris gegevensbescherming (FG) in samenwerking met de chief information security officer (CISO). De FG en/of de CISO kunnen het datalekregister ook gebruiken om te monitoren of voorgenomen verbetermaatregelen tijdig worden geïmplementeerd. Het is dan wel van belang dat het datalekregister compleet is en zorgvuldig wordt bijgehouden.

Rol van de FG

De meeste instellingen (twaalf van de vijftien) betrekken de FG actief bij de afhandeling van datalekken. De overige drie instellingen betrekken de FG geheel niet volgens hun interne beleid. In één geval was het beleid zo ingericht dat de FG het besluit nam of de instelling een datalek moest melden aan de AP en de slachtoffers van het datalek. Zo'n rol is echter niet verenigbaar met de onafhankelijke positie van de FG. FG's kunnen geen goed toezicht houden op de naleving van de Algemene verordening gegevensbescherming (AVG) als zij zelf een actieve rol hebben bij de uitvoering van AVG-verplichtingen, zoals de meldplicht datalekken. Deze uitvoerende taken kunnen wel belegd worden bij bijvoorbeeld de Privacy Officer.

Meldbeleid is soms verouderd

Ook hebben de meeste instellingen (elf van de vijftien) het interne meldbeleid recentelijk geëvalueerd of vernieuwd. Vier instellingen hebben het beleid sinds 2020 niet meer geëvalueerd of vernieuwd. Uit de afgenomen interviews bleek dat dit ertoe kan leiden dat het proces in de praktijk afwijkt van het vastgestelde meldbeleid. Dit kan zorgen voor onduidelijkheid over de rolverdeling, met name bij hoog verloop van de betrokken medewerkers, wat bij veel jeugdzorginstellingen voorkomt.

3. Datalekregister

3.1 Belang van het datalekregister

Het is van belang om alle datalekken te documenteren, ongeacht of organisaties een datalek aan de AP melden, om analyses uit te kunnen voeren die een compleet beeld weergeven. Daarnaast is het cruciaal om de betrokken jeugdzorgcliënten beter te kunnen beschermen voor de mogelijke gevolgen. Bovendien is het een onderdeel van de verantwoordingsplicht uit de AVG.[8] Organisaties moeten alle bijzonderheden over elk datalek registreren. Zoals de oorzaak, wat er precies is gebeurd, om welke persoonsgegevens het gaat, wat de gevolgen van het datalek zijn en welke corrigerende maatregelen de organisatie heeft genomen. Zo kunnen organisaties aantonen dat zij datalekken melden aan de AP en aan de slachtoffers wanneer dat nodig is.

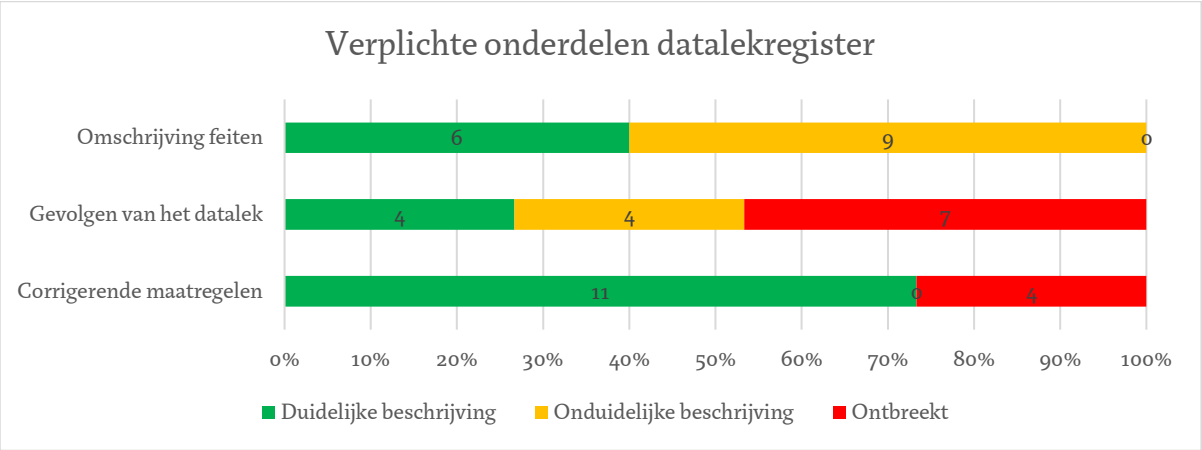
Het is echter belangrijk dat organisaties het datalekregister bijhouden niet uitsluitend als een administratieve verplichting zien, maar vooral als middel om te leren van eerdere incidenten. Organisaties kunnen het datalekregister gebruiken om te reflecteren op eerdere fouten, de effectiviteit van

[8] Zie ook: Richtsnoeren 9/2022, p. 30 en 31.

beveiligingsmaatregelen te beoordelen en waar nodig verbeteringen door te voeren. Daarmee kan het register een belangrijke bijdrage leveren aan betere bescherming van persoonsgegevens.

3.2 Beoordeling datalekregisters

De AP heeft aan vijftien jeugdzorginstellingen gevraagd om hun datalekregister[9] te verstrekken, met alle registraties vanaf 1 januari 2020 tot en met 30 april 2024. De AP heeft onder meer beoordeeld of deze datalekregisters de wettelijk verplichte onderdelen bevatten: een duidelijke omschrijving van de feiten, de gevolgen van het datalek en de genomen corrigerende maatregelen. Het resultaat staat in deze tabel:



Bij de beoordeling van de opgevraagde datalekregisters viel een aantal zaken op. Sommige registers bevatten slechts zeer summiere informatie en onduidelijke omschrijvingen. Deze registers waren in een aantal gevallen ook incompleet en/of bevatten niet alle wettelijk verplichte onderdelen, zoals de gevolgen van het datalek en de genomen corrigerende maatregelen. Omdat deze registers onduidelijk of incompleet waren, kon de AP niet goed beoordelen in hoeverre de betreffende instellingen datalekken melden aan de AP en aan de slachtoffers wanneer dat nodig is. De onvolledigheid van deze registers maakt het daarnaast voor de betreffende instellingen lastig om goed te rapporteren over datalekken aan de stakeholders binnen de organisatie en om de effectiviteit van eerdere maatregelen te evalueren.

Omschrijving van de feiten

De AP kwam in verschillende datalekregisters zeer korte en onduidelijke omschrijvingen tegen van datalekken. Een voorbeeld hiervan is:

- *"Per ongeluk stukken gemaild naar de advocaat die nog geregistreerd stond maar inmiddels is deze vervangen door de moeder."*

Door het gebruik van afkortingen en korte omschrijvingen van de feiten, is niet altijd duidelijk wat voor soort persoonsgegevens zijn geraakt. De betreffende instelling kan daardoor achteraf niet nagaan of een goede afweging is gemaakt over de ernst van het datalek en de consequenties ervan. Daarnaast kan (achteraf) het bestuur en/of de AP niet goed beoordelen of een juiste risico-inschatting is gemaakt van de mogelijke gevolgen van het datalek voor de slachtoffers, en of het datalek terecht wel of niet is gemeld aan de AP en aan de slachtoffers.

Omschrijving van de gevolgen

De AP kwam in vier registers onduidelijke omschrijvingen van de gevolgen van een datalek tegen. Bijvoorbeeld dat er sprake is van een 'verwaarloosbaar', 'laag', 'midden', of 'hoog' risico, zonder uitleg waarom een datalek in een bepaalde risicocategorie valt. Als de gevolgen van het datalek niet duidelijk zijn

[9] Het gaat daarbij om de documentatie zoals bedoeld in artikel 33, vijfde lid, AVG.

beschreven, kan de betreffende instelling achteraf niet beoordelen of de juiste corrigerende maatregelen zijn genomen. Ook kan de AP hierdoor achteraf niet goed beoordelen of de beslissing terecht is geweest om het datalek wel of niet te melden aan de AP en aan de slachtoffers.

Verder zijn in zeven van de vijftien datalekregisters de gevolgen van het datalek niet apart omschreven. De gevolgen van het datalek zijn soms wel af te leiden uit de beschrijving van het incident. Toch is het belangrijk om de gevolgen van het datalek apart op te nemen in het datalekregister, zoals de AVG voorschrijft. Dezelfde inbreuk kan namelijk in de ene situatie ingrijpender gevolgen hebben dan in de andere.

Corrigerende maatregelen

Bij vier van de vijftien datalekregisters zijn de corrigerende maatregelen niet geregistreerd. Sommige instellingen registreren alleen de genomen preventieve maatregelen om nieuwe datalekken te voorkomen, maar vermelden niet of het datalek is beëindigd en zo ja, hoe. Daardoor kan de instelling (en de AP) achteraf niet goed beoordelen of genoeg is gedaan om de negatieve gevolgen voor de slachtoffers te beperken. Het is dan onduidelijk of het datalek nog voortduurt of al is beëindigd. Bij een verkeerd verstuurd poststuk is het dan bijvoorbeeld niet duidelijk of de brief door de onjuiste ontvanger is vernietigd of geretourneerd, en dus of de inbreuk beëindigd is of nog voortduurt.

Aanbeveling: Zorg voor een duidelijke en volledige datalekregistratie

Om datalekken goed te kunnen afhandelen, en dit ook te kunnen aantonen, is het belangrijk dat uw datalekregister in ieder geval de wettelijk verplichte onderdelen bevat: een duidelijke omschrijving van de feiten, de gevolgen van het datalek en de genomen corrigerende maatregelen. Registreer deze onderdelen afzonderlijk. Zorg er vooral voor dat uit de omschrijving van een datalek duidelijk blijkt wat er is gebeurd. Benoem in ieder geval: de oorzaak van het datalek, wat zich heeft afgespeeld, welke groep(en) slachtoffers is/zijn getroffen en om wat voor soort persoonsgegevens het gaat. Zo kunt u achteraf nagaan of u een goede risico-inschatting heeft gemaakt.

Daarnaast adviseert de AP om deze onderdelen ook op te nemen in uw datalekregister:

- de maatregelen die u heeft genomen om nieuwe, soortgelijke datalekken te voorkomen;
- of u het datalek wel of niet gemeld heeft aan de AP en aan de slachtoffers;
- waarom u het datalek wel of niet gemeld heeft aan de AP en aan de slachtoffers;
- als u een datalek te laat heeft gemeld aan de AP: waarom dat zo is.
- Bovendien is het van belang om het register regelmatig te analyseren en minstens twee keer per jaar te rapporteren aan het bestuur over de datalekken in de afgelopen periode.

Voorbeeld van datalekregister

Om organisaties op weg te helpen, heeft de AP een voorbeeld van een datalekregister gemaakt.
Dit voorbeeld is te downloaden via de website van de AP:
https://autoriteitpersoonsgegevens.nl/documenten/voorbeeld-datalekregister

3.3 Bad practices

De AP ziet bij meerdere van de onderzochte jeugdzorginstellingen twee 'bad practices'.

Datalekregister bevat ook andersoortige incidenten

Een aantal instellingen maakt gebruik van één register voor verschillende soorten incidenten. In dit register registreren zij ook andere beveiligingsincidenten dan datalekken, zoals fysieke incidenten en incidenten waarbij geen persoonsgegevens betrokken zijn. Hierdoor is minder makkelijk terug te vinden hoeveel datalekken binnen een bepaalde periode hebben plaatsgevonden bij de betreffende instelling. Dit maakt het intern en extern rapporteren over datalekken en het evalueren van genomen maatregelen lastiger.

De AP raadt daarom aan om datalekken altijd (ook) in een apart daarvoor bedoeld register vast te leggen.

Ongeschikte softwaresystemen gebruikt als datalekregister

Een aantal instellingen maakt gebruik van aparte systemen voor het vastleggen van meldingen over incidenten, waaronder datalekken. Dit zijn systemen die zijn ingericht op het beheren en afhandelen van meldingen ('tickets'). Sommige instellingen gebruiken deze systemen ook als intern datalekregister, terwijl de systemen daarop niet goed zijn ingericht. Tijdens het onderzoek heeft de AP ervaren dat instellingen moeite hebben om de datalekregistraties uit deze systemen te exporteren en bij de AP aan te leveren. Deze exports bevatten daarnaast veel overbodige informatie, zoals persoonsgegevens van de initiële melder van het datalek en de namen van de medewerkers die de melding behandeld hebben. Daarmee is het voor de betreffende instellingen moeilijk om een goed overzicht te krijgen van het soort en het aantal datalekken dat plaatsvindt binnen de instelling en om de effectiviteit van de genomen maatregelen te beoordelen.

De AP raadt daarom aan om een apart systeem of overzicht te gebruiken voor het registreren van datalekken, dat makkelijk doorzoekbaar is en eenvoudig te exporteren. Ook kan gekozen worden voor een systeem dat een koppeling kan maken met het aanwezig verwerkingsregister, zodat eenvoudig is te achterhalen bij welke verwerking het datalek zich heeft voorgedaan en welke gevolgen het datalek kan hebben (welke soorten persoonsgegevens en groepen betrokkenen worden geraakt).

3.4 Andere opvallende zaken

Naast de genoemde bad practices vielen de AP enkele andere zaken op.

Meer datalekken gemeld bij de AP dan vastgelegd in datalekregister

Bij vijf jeugdzorginstellingen kwam het aantal datalekken dat volgens het datalekregister gemeld was aan de AP, niet overeen met het aantal meldingen dat de AP daadwerkelijk ontving. Alle instellingen meldden meer datalekken aan de AP dan zij in het register aangaven. Een aantal meldingen dat de AP heeft ontvangen, was bovendien niet terug te vinden in het datalekregister van de betreffende instelling. Melden organisaties datalekken wel aan de AP, maar registreren zij die niet in hun eigen datalekregister? Dan kunnen zij achteraf niet goed nagaan of er verbetermaatregelen zijn genomen. Ook kunnen zij dan op basis van het register niet goed rapporteren over het aantal datalekken in een bepaalde periode.

Veelvoorkomend type datalek: verkeerd verstuurde e-mails en post

Een brief of e-mail met persoonsgegevens die terechtkomt bij de verkeerde ontvanger, is een veelvoorkomend datalek bij jeugdzorginstellingen. Een dossier wordt bijvoorbeeld per ongeluk naar de verkeerde persoon gemaild. Of een brief wordt verstuurd naar het verkeerde adres, omdat een verhuizing niet goed is doorgevoerd. Bij dit soort datalekken is het van belang om de gevolgen voor de slachtoffers te benoemen in het register, omdat de gevolgen per situatie sterk kunnen verschillen. Ook is het belangrijk om bij te houden hoe nieuwe incidenten worden voorkomen.
De AP beveelt aan om daarbij onder meer na te denken over deze vragen:

- Is het een optie om de gevoelige documenten persoonlijk te overhandigen in plaats van deze per post of e-mail te versturen?
- Als het document digitaal moet worden verstuurd: kan er gebruikgemaakt worden van een beveiligd e-mailsysteem of een veilige online portal?

4. Beveiligingsmaatregelen en bewustwording

4.1 Beveiligingsmaatregelen

Alle instellingen die de AP heeft onderzocht, hebben software om beveiligd e-mails te versturen. Door menselijke fouten komt het echter nog steeds voor dat medewerkers e-mails verkeerd versturen. Uit de afgenomen interviews blijkt dat dit soms komt doordat medewerkers de beveiligde mailsystemen als onpraktisch ervaren en die daardoor niet (altijd) gebruiken. Wanneer beveiligde e-mailsystemen of online portals gebruiksvriendelijk zijn, is het eenvoudiger en laagdrempeliger voor medewerkers om daar gebruik van te maken.

4.2 Bewustwording medewerkers

Een aantal instellingen doet er nog niet genoeg aan om medewerkers goed bewust te maken van het belang van naleving van de AVG. Datalekken moeten zoveel mogelijk worden voorkomen. En als er datalakken zijn dan moeten deze kunnen worden herkend en zorgvuldig worden afgehandeld. Sommige instellingen besteden alleen aandacht aan dit thema tijdens de 'onboarding' van nieuwe medewerkers (bijvoorbeeld met een privacychecklist), maar organiseren daarna geen aanvullende trainingen of bewustwordingssessies meer. Herhaling van dit thema is echter belangrijk in verband met verloop van medewerkers.

Weten medewerkers niet hoe ze een datalek moeten herkennen? En zijn ze niet op de hoogte van het interne meldbeleid? Dan ontstaat het risico dat datalekken onopgemerkt blijven en niet intern worden gemeld en geregistreerd. Daardoor melden instellingen datalekken die zij zouden moeten melden mogelijk ook niet aan slachtoffers en aan de AP. Worden datalekken onterecht niet aan de AP gemeld? Dan kan de AP niet controleren of de slachtoffers goed zijn geïnformeerd en of de genomen corrigerende maatregelen in orde zijn.

Aanbeveling: Besteed aandacht aan bewustwording onder medewerkers

Zorg ervoor dat uw medewerkers weten wat een datalek is. En wat ze moeten doen wanneer ze een datalek ontdekken of veroorzaken. Zo voorkomt u dat datalekken onopgemerkt blijven en niet intern worden gemeld en geregistreerd. Alleen met een compleet register is een analyse van alle datalekken mogelijk, waardoor de bescherming van persoonsgegevens van jeugdzorgcliënten verbeterd kan worden. Goede zorg voor jeugdzorgcliënten houdt ook in dat voor hun persoonsgegevens gezorgd wordt. Als niet alle datalekken intern gemeld en geregistreerd worden, dan loopt u het risico dat u datalekken ten onrechte niet meldt aan slachtoffers en aan de AP . En u dus de AVG overtreedt. Besteed hieraan aandacht bij de 'onboarding' van nieuwe medewerkers, bespreek/evalueer datalekken binnen het team waar ze plaatsvinden en organiseer regelmatig trainingen, workshops en awareness-campagnes. Het is belangrijk om niet alleen bij nieuwe werknemers hiervoor aandacht te vragen, maar om dit thema te blijven herhalen. Bijvoorbeeld met een verplichte jaarlijkse e-learning.

BIJLAGE - Lering trekken uit eerdere datalekken (Plan-Do-Check-Act)

Het is belangrijk dat organisaties het datalekregister bijhouden niet uitsluitend als een administratieve verplichting zien, maar ook als middel om te leren van eerdere incidenten. De AP geeft hierbij een voorbeeld van een stappenplan dat organisaties periodiek kunnen uitvoeren als onderdeel van de Plan-Do-Check-Act (PDCA-)cyclus. Dit stappenplan kunnen zij gebruiken om bij te houden of (bepaalde typen) datalekken toenemen, wat daar de mogelijke oorzaak van is, of eerder genomen maatregelen hebben gewerkt om het aantal datalekken te verminderen en of er aanvullende maatregelen nodig zijn. Zo kunnen organisaties de beveiliging van persoonsgegevens voortdurend evalueren en verbeteren.

STAP 1: Maak een analyse op basis van het datalekregister

- Hoeveel datalekken hebben de afgelopen periode plaatsgevonden?
- Om wat voor type datalekken ging het? Welke type datalekken komt het meest voor?
- Welke type datalekken levert het hoogste risico op voor slachtoffers?

Vergelijk met voorgaande perioden: zijn er opvallende trends zichtbaar?

- Is het aantal (ernstige) datalekken toegenomen of afgenomen?
- Zijn er de afgelopen periode meer datalekken gemeld aan de AP en aan de slachtoffers?
- Is er een toename of afname zichtbaar in bepaalde type datalekken?
- Wat is de mogelijke oorzaak van de toename of afname?

Let op: toename of afname in het aantal (gemelde) datalekken kan ook zijn veroorzaakt doordat in de afgelopen periode intern meer of minder datalekken zijn gemeld/geregistreerd dan daarvoor.

STAP 2: Bekijk welke maatregelen u kunt nemen om het risico op de ernstigste en/of veelvoorkomende datalekken te beperken

Geef prioriteit aan maatregelen gericht tegen datalekken die het hoogste risico opleveren, en aan relatief eenvoudig te nemen maatregelen die waarschijnlijk direct effect zullen hebben ('laaghangend fruit').

STAP 3: Monitor de implementatie van de voorgenomen (aanvullende) beveiligingsmaatregelen

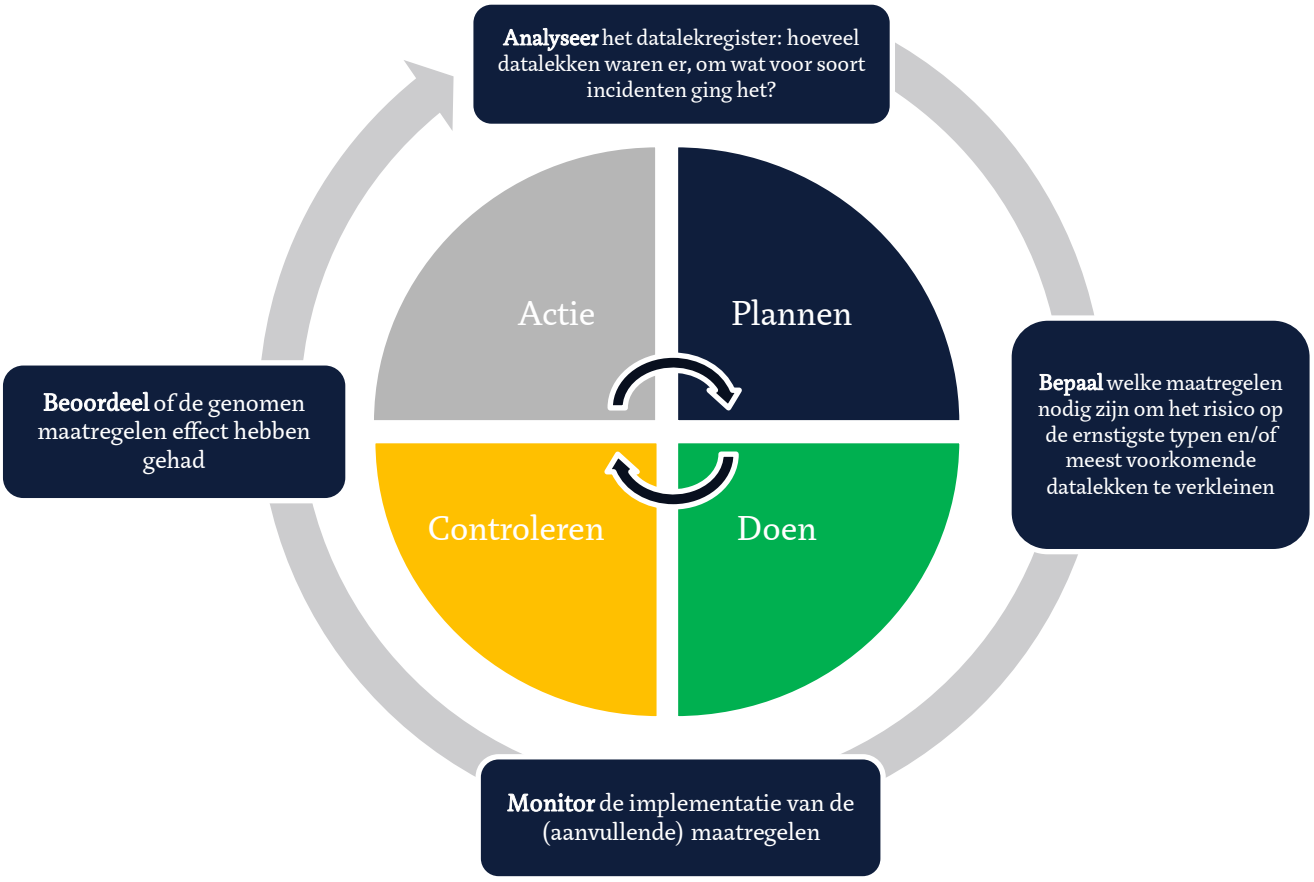
- Zijn de aangekondigde maatregelen uit de vorige cyclus inmiddels ingevoerd?
- Zo niet, hoe komt dat? Wanneer worden deze maatregelen alsnog uitgevoerd?

Zijn voorgenomen beveiligingsmaatregelen niet binnen de afgesproken periode geïmplementeerd? Spreek het verantwoordelijke management hierop aan en maak hierover afspraken.

STAP 4: Beoordeel (bijvoorbeeld: na een half jaar) of de genomen aanvullende maatregelen effect hebben gehad

- Hebben de maatregelen die tijdens de vorige cyclus zijn ingevoerd geleid tot een afname van het aantal datalekken (van een bepaald type)?
- Als de maatregelen niet effectief zijn gebleken, waar lag dat aan? Zijn er aanvullende maatregelen nodig?

Herhaal de stappen 1 t/m 4 elk jaar of elk half jaar en rapporteer hierover aan het hoogste management. De AP raadt aan om de FG en de CISO te betrekken bij de uitvoering van deze stappen.


Analyseer het datalekregister: hoeveel datalekken waren er, om wat voor soort incidenten ging het?
Plannen
Doen
Controleren
Actie
Bepaal welke maatregelen nodig zijn om het risico op de ernstigste typen en/of meest voorkomende datalekken te verkleinen
Monitor de implementatie van de (aanvullende) maatregelen
Beoordeel of de genomen maatregelen effect hebben gehad