Update boek Grip op Datalekken:
Definitieve beleidsregels meldplicht datalekken

In het boek Grip op datalekken zijn de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens (AP) opgenomen. Dit is gebeurd op basis van de consultatie-versie. In december 2015 zijn de definitieve beleidsregels gepubliceerd.

In voorliggend overzicht lees je waar de definitieve beleidsregels afwijken van die uit de consultatieversie. We geven eerst een overzicht en leggen daaropvolgend de aandachtspunten per stuk uit.

1. Meldenswaardige datalekken moeten uiterlijk binnen 72 uur na ontdekking worden gemeld bij de Autoriteit Persoonsgegevens.

2. Het maximum boetebedrag is (door de tweejaarlijkse indexatie van Wetboek van Strafrecht) verhoogd naar 820.000 euro.

3. De Autoriteit Persoonsgegevens geeft extra uitleg over cryptografische verwerkingen. Onder bepaalde omstandigheden kan adequate versleuteling ertoe leiden dat je een datalek niet hoeft te melden aan betrokkenen.

4. Specifieke afspraken over het melden van een datalek door de bewerker hebben nu de voorwaarde dat het duidelijk moet zijn onder welke omstandigheden de bewerker zélf de melding moet doen bij de toezichthouder.

5. Het verschil tussen een beveiligingslek, beveiligingsincident en een datalek is geconcretiseerd. Alleen als er meer dan een dreiging is geweest, kwalificeert het als beveiligingsincident in plaats van een beveiligingslek. Het is slechts een datalek als er bij de inbreuk op de beveiliging persoonsgegevens verloren zijn gegaan of een onrechtmatige gegevensverwerking niet redelijkerwijs is uit te sluiten. De Autoriteit Persoonsgegevens stipt ook de omvang van een meldenswaardig datalek aan: het kan voorkomen dat bij één betrokkene het datalek ernstige gevolgen heeft en dus meldenswaardig is. Aansluitend geeft de toezichthouder nieuwe voorbeelden van niet-meldenswaardige datalekken.

6. Er wordt extra nadruk gelegd op de (eigen) verantwoordelijkheid voor het doen van de melding(en), voor het zelf uitzoeken van de oorzaak van het datalek en het nemen van passende maatregelen ter voorkoming ervan.

7. Tot slot schrijft de AP in de definitieve beleidsregels dat wanneer je de opdracht krijgt alsnog betrokkene(n) over een datalek te informeren, dit een bindende aanwijzing is. Het niet opvolgen van een bindende aanwijzing kan leiden tot een (dus verhoogde) maximale boete van 820.000 euro.

Hoe snel moet je melden?

De meest concrete verandering is de termijn waarbinnen je de melding moet doen. In de consultatieversie was dit 'uiterlijk op de tweede werkdag na de ontdekking'. Daarbij werd rekening gehouden met weekenden, feestdagen en daaraan gelijkgestelde dagen. In navolging van de aankomende Europese Algemene Verordening Gegevensbescherming is de termijn nu 72 uur na de ontdekking. Indien je de 72 uur niet haalt, dien je dit te motiveren. Dit heeft directe consequenties voor de planning. Mocht je nou een datalek ontdekken op een vrijdagmiddag of een dag voor kerst, dan is het dus nog even doorzetten.

Wat is de maximale boete?

Een andere verandering op concreet niveau is de hoogte van de bestuurlijke boete die de AP kan uitdelen. Het maximum is met 10.000 euro verhoogd. Dat betekent dat je bijvoorbeeld bij falend privacymanagement of het niet nakomen van een bindende aanwijzing een boete kunt krijgen van 820.000 euro. Dit komt omdat de bedragen van bestuurlijke boetes, te vinden in het Wetboek van Strafrecht, iedere twee jaar worden aangepast aan de ontwikkeling van de consumentenprijsindex. Dat betekent dat het maximale boetebedrag in 2018 weer anders kan zijn.

Cryptografie

In de definitieve beleidsregels Meldplicht Datalekken heeft de AP meer aandacht voor het toepassen van cryptografische verwerkingen (als beveiligingsmaatregel) op identificerende gegevens die leiden tot pseudonimisering. Hierbij benadrukt de AP dat voor zover het nog mogelijk is om betrokkenen te identificeren er nog steeds sprake is van persoonsgegevens. Zo verduidelijkt de AP dat het verwijderen van de direct identificerende gegevens (als beveiligingsmaatregel) op zichzelf niet altijd voldoende garantie biedt om ervoor te zorgen dat er geen sprake meer is van persoonsgegevens. Aansluitend benadrukt de toezichthouder dat je bij het anonimiseren van persoonsgegevens rekening moet houden met de stand van de techniek.

De AP beantwoordt in een nieuwe paragraaf de vraag "*Biedt de cryptografie die ik heb toegepast voldoende bescherming om de melding aan de betrokkene achterwege te laten?*". Daarin staat de technische maatregel om persoonsgegevens onbegrijpelijk of ontoegankelijk te maken voor onbevoegden centraal. Er is ook extra aandacht voor encryptie (versleuteling) en hashing (het omzetten van gegevens in unieke code). De AP legt uit dat cryptografische bewerkingen die zodanig zijn toegepast dat uitgelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden je geen melding hoeft te doen van het datalek aan betrokkenen.

Ook wijst de AP erop dat beide beveiligingsmethoden encryptie en hashing te 'kraken' zijn (wanneer onbevoegden toegang krijgen tot de gegevens). Daarnaast geeft ze extra beveiligingstips mee om het kraken tegen te gaan, o.a. door het gebruik van moderne cryptografische technieken. De AP benadrukt dat technieken verouderen en dat daarom periodieke beoordeling van de beveiligingsmaatregelen en (waar nodig) updates noodzakelijk zijn.

De AP beschrijft in de definitieve versie van de beleidsregels drie aandachtspunten voor de beoordeling van adequaat versleutelde persoonsgegevens:

- kwetsbaarheden van het algoritme of de wijze waarop deze is toegepast welke de mate van beveiligingsmaatregelen beïnvloedt;
- de mogelijkheid tot (ongeautoriseerde) de-encryptie van persoonsgegevens;
- de mogelijkheid tot het (herhaaldelijk) toepassen van de gebruikte hashingmethodes, kan leiden tot inbreuk op de beveiliging.

In de conceptversie beleidsregels stelde de AP al dat een beoordeling van een externe deskundige uitsluitsel kan bieden over het juist toepassen van een algoritme of adequate versleuteling. In de definitie versie voegt ze hieraan toe dat dit oordeel bij voorkeur plaats moet vinden vóórdat er sprake is van een datalek. Voor een adequate versleuteling van persoonsgegevens vestigt de AP de aandacht op het voorkomen van uitlekken van encryptie-sleutels en zogenaamde 'salts'.

Bewerker: afspraken en toezicht

Het was reeds bekend dat ook de bewerker de eerste melding van een datalek kan doen bij de AP. In de definitieve versie is het 'maken van afspraken' met de bewerker iets formeler aangezet. De AP gebruikt daarvoor nu het woord 'overeenkomen'. Daarnaast heeft de AP een voorwaarde toegevoegd waaronder de bewerker de eerste melding op zich kan nemen. De bewerker moet dan, op basis van de afspraken die zijn overeengekomen, kunnen overzien in welke gevallen een melding aan de AP noodzakelijk is.

Met betrekking tot het toezicht op de bewerker heeft de AP verduidelijkt dat het 'recht van die lidstaat' betrekking heeft op de lokale verplichtingen op het gebied van informatiebeveiliging. Je dient als verantwoordelijke dus de naleving van beveiligingsmaatregelen te waarborgen in een bewerkersovereenkomst conform de definities van de wetgeving van de lidstaat waarin de bewerker is gevestigd.

Beveiligingslek, beveiligingsincident en datalek

De definitie van een datalek is geconcretiseerd door de AP door twee situaties die nog geen datalek zijn te benoemen: een beveiligingslek en een beveiligingsincident. Deze verheldering leidt tot andere vragen dan in het stroomschema van de concept richtsnoeren Meldplicht Datalekken. De vraag in het conceptschema die moest helpen bij het bepalen of er sprake is van een datalek: "*Zijn de verwerkte persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking*" is opgesplitst en uitgebreid met de vragen "*Is er sprake van een inbreuk op de beveiliging*", "*Zijn bij de inbreuk persoonsgegevens verloren gegaan*" en "*Kan ik redelijkerwijs uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt?*".

In een nieuw schema legt de AP uit dat er een verschil is tussen een beveiligingslek, een beveiligingsincident en een datalek. Ze verduidelijkt ook enkele categorieën maatregelen uit artikel 13 Wbp (beveiliging). Hiernaast specificeert en benadrukt de AP dat er pas sprake is van een inbreuk op de beveiliging wanneer er zich daadwerkelijk een beveiligingsincident heeft voorgedaan en de eventuele preventieve maatregelen die je hebt genomen dit niet konden voorkomen. Bij een beveiligingslek is er dus slechts sprake van een dreiging.

Aansluitend geeft de AP aan dat het kenmerkend is voor een datalek dat het beveiligingsincident daadwerkelijk gevolgen heeft voor de persoonsgegevens die door jou worden verwerkt. Hierbij gaat het dan om het verlies van persoonsgegevens of het niet redelijkerwijs kunnen uitsluiten van onrechtmatige verwerking van persoonsgegevens. De repressieve – en herstelmaatregelen die je eventueel hebt getroffen blijken in dat geval volgens de AP dus onvoldoende om deze gevolgen geheel weg te nemen.

Verlies van persoonsgegevens en back-up

De AP stelt in de definitieve beleidsregels Meldplicht Datalekken dat er ook sprake is van verlies wanneer je (bij verlies) niet beschikt over een complete en actuele reservekopie van de gegevens. De AP benadrukt dat onder deze omstandigheden er sprake is van een datalek.

(Omvang van een) meldenswaardig datalek

Met betrekking tot de omvang van een datalek schrijft de AP in de definitieve versie van de beleidsregels Meldplicht Datalekken dat ook waar de betrokkene slechts één persoon betreft, de meldplicht van toepassing is. Hiernaast noemt de AP de volgende nieuwe voorbeelden die illustreren wanneer de meldplicht niet van toepassing is:

- foutief geadresseerde brieven komen ongeopend retour.
- verloren koffer met goed slot komt ongeopend terug bij rechtmatige eigenaar.
- ledenadministratie van een algemene sportvereniging raakt zoek of is gehackt (tenzij de vereniging richt op specifieke levensovertuigingen of geaardheid of gegevens fraudegevoelig zijn).
- ongeautoriseerde toegang tot medische persoonsgegevens door ziekenhuispersoneel middels gebruik van het wachtwoord van een arts (dit is in eerste instantie meer een schending van interne voorschriften dan een datalek).

Het afhandelen van de meldingen door AP

De AP heeft in de definitieve beleidsregels expliciet aangegeven dat de verantwoordelijkheid om de oorzaak van het datalek te vinden en maatregelen te treffen om te voorkomen dat het datalek nog een keer zal plaatsvinden bij de verantwoordelijke ligt. Je zal ook zelf moeten bepalen of en op welke manier je betrokkenen wilt informeren. De beleidsregels zullen je ondersteunen bij het maken van deze overwegingen, maar de AP zal hierbij geen ondersteuning bieden.

De AP heeft in de definitieve beleidsregels gespecificeerd dat, waar ze van je verlangt de betrokkene(n) alsnog te informeren over het datalek, deze opdracht een bindende aanwijzing is. Wanneer je dan niet overgaat tot het informeren van betrokkene(n) kun je een bestuurlijke boete krijgen van de hoogste categorie (maximaal 820.000 euro). De AP wil via de meldingen strikt toezien op de transparantie tegenover betrokkenen over datalekken die hen persoonlijk raken of waarvan zij last kunnen ondervinden. Ook kan de AP op basis van de meldingen actie te ondernemen om de adequate beveiliging van persoonsgegevens te bevorderen. Zo kan ze overgaan tot een onderzoek naar de naleving van de beveiligingsverplichtingen uit de Wbp binnen de organisatie.