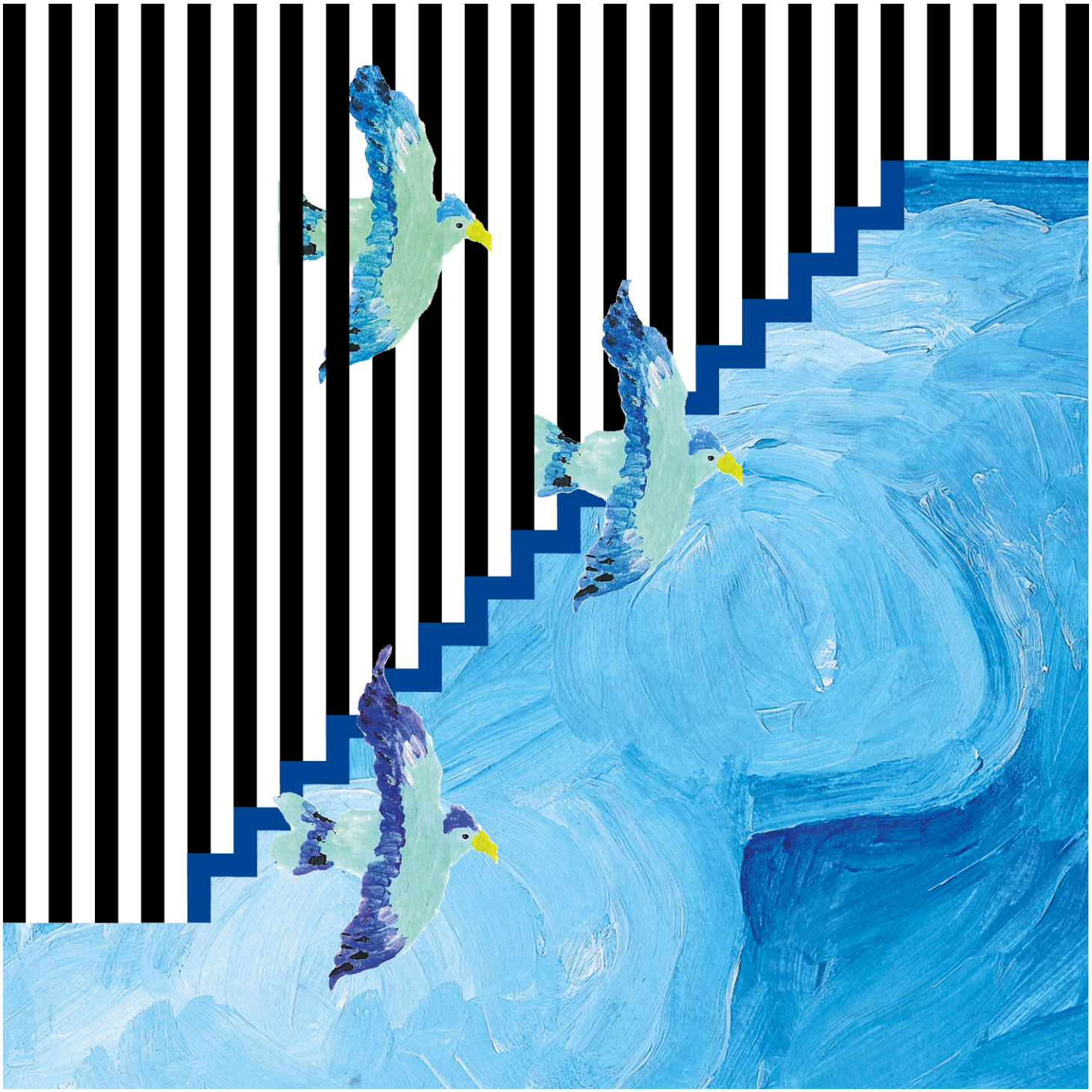

Samenvatting van de richtsnoeren van het College bescherming persoonsgegevens voor de Wet meldplicht datalekken

Kennedy Van der Laan

Op 1 januari 2016 treedt de Wet Meldplicht Datalekken in werking. Het CBP heeft op 21 september Richtsnoeren gepubliceerd ter verduidelijking van bepaalde aspecten van de nieuwe meldplicht datalekken. Hieronder vindt u een samenvatting van deze Richtsnoeren.

Het is het belangrijk op te merken dat deze versie van de Richtsnoeren door het CBP nog gebruikt wordt voor openbare raadpleging. Niet alleen kunnen bepaalde dingen nog wijzigen, het CBP vraagt ook actief om feedback van bedrijven die zullen moeten voldoen aan deze Richtsnoeren. Als u een reactie wilt indienen bij het CBP helpen wij u daar uiteraard graag bij. Reacties dienen uiterlijk op 19 oktober 2015 binnen te zijn.

1. De voorbereiding

De Richtsnoeren maken duidelijk dat de verantwoordelijke ervoor moet zorgen dat zijn bewerkers hem in staat stellen om zijn wettelijke verplichtingen na te komen. Dit betekent in ieder geval dat de bewerker u tijdige en adequate informatie moet geven over de datalekken waarvan hij kennis krijgt. Daartoe moet de verantwoordelijke een schriftelijke overeenkomst aangaan met zijn bewerker, waarin de volgende punten staan:

1. De bewerker zal de verantwoordelijke informeren over relevante incidenten. Partijen moeten een plan opstellen dat beschrijft hoe de verantwoordelijke zal worden geïnformeerd en op de hoogte gehouden gedurende de tijd die het oplossen van het datalek in beslag neemt.
2. Hoe snel moet de verwerker de verantwoordelijke waarschuwen?
3. Wie doet de eerste melding aan het CBP? De verantwoordelijke of de bewerker? Het CBP vindt blijkbaar niet dat het altijd de verantwoordelijke moet zijn die de melding doet. Deze melding kan later worden aangevuld door de verantwoordelijke, die waarschijnlijk meer informatie heeft over de betrokkenen die met het lek te maken hebben.
4. De verwerker dient maatregelen te nemen om incidenten te voorkomen en datalekken op te sporen, bijvoorbeeld met *intrusion detection systems*.
5. Is er een manier om te controleren of de verwerker voldaan heeft aan zijn verplichtingen om de verantwoordelijke te informeren en op de hoogte te houden?

Wij merken op dat het CBP twee verrassende dingen zegt over verantwoordelijken, waardoor enige verwarring ontstaat over hun rol.

1. Het CBP zegt dat hoewel de verantwoordelijke verantwoordelijk en aansprakelijk is voor nakoming, de bewerker ook verantwoordelijk is voor nakoming. Hij mag niet alleen maar de instructies van de verantwoordelijke volgen, maar moet zijn eigen verantwoordelijkheid nemen voor de nakoming van de eisen als bepaald in gegevensbeschermingswetgeving. Dit is in lijn met een recent rapport dat het CBP heeft gepubliceerd, maar het is strijdig met de geaccepteerde uitleg van de wet. Bovendien druist het in tegen uitlatingen van de overheid dat verplichtingen in de Wbp worden opgelegd aan de verantwoordelijke (en niet aan anderen).
2. Het CBP zegt ook dat de verantwoordelijke erop moet toezien dat de bewerker voldoet aan zijn verplichtingen plaatselijk recht. Het CBP verwijst naar artikel 14 lid 4 van de Wet Bescherming Persoonsgegevens (een implementatie van artikel 17 lid 3 onder 2 van de Richtlijn Gegevensbescherming). Die Richtlijn is echter heel duidelijk dat deze verplichting niet van toepassing is op al het plaatselijk recht, maar alleen op de verplichtingen ten aanzien van informatiebeveiliging. Naar onze mening gebruikt het CBP een ongelukkige vertaling in de Nederlandse implementatie van de Richtlijn om de reikwijdte van deze verplichting groter te maken dan de wetgever heeft bedoeld.

2. Melden of niet?

Is het incident een datalek?

Deze vraag moet in twee delen worden beantwoord:

1. *Zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking?*

De verantwoordelijke moet eerst de vraag beantwoorden of er inbreuk is gemaakt op zijn technische en organisatorische beveiligingsmaatregelen. Het is niet relevant of de verantwoordelijke passende technische en organisatorische beveiligingsmaatregelen had getroffen om verlies of onrechtmatige verwerking te voorkomen. Het enige wat ertoe doet is of er een inbreuk is geweest. De verantwoordelijke moet bijvoorbeeld aannemen dat de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking in geval van een malware-besmetting.

2. *Kan de verantwoordelijke uitsluiten dat er persoonsgegevens daadwerkelijk verloren zijn gegaan of onrechtmatig zijn verwerkt?*

De tweede vraag is of de verantwoordelijke redelijkerwijs kan uitsluiten dat er daadwerkelijk gegevens zijn verloren gegaan of onrechtmatig zijn verwerkt. Als de gegevens bijvoorbeeld zijn vernietigd maar via een back-

up weer konden worden hersteld is het incident geen datalek. Wanneer de verantwoordelijke ontdekt dat een werknemer zijn gebruikersnaam en wachtwoord aan een derde heeft gegeven, maar door middel van logbestanden kan vaststellen dat niemand deze gegevens heeft gebruikt om in te loggen, is het incident ook geen datalek.

3. Melden aan het CBP

De verantwoordelijke moet een melding doen aan het CBP wanneer het datalek (waarschijnlijk) ernstige nadelige gevolgen zal hebben voor de bescherming van persoonsgegevens. Dit zal altijd het geval zijn indien de gegevens van gevoelige aard zijn.

Gevoelige gegevens worden gedefinieerd als ten minste:

- Bijzondere categorieën persoonsgegevens (persoonlijke gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen).
- Gegevens over de financiële of economische situatie van de betrokkene.
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting.
- Gebruikersnamen, wachtwoorden en andere inloggegevens.
- Gegevens die kunnen worden misbruikt voor identiteitsfraude.

Indien de gegevens niet in deze categorieën vallen kan het incident nog steeds ernstige nadelige gevolgen hebben vanwege de aard en omvang van het datalek. De volgende overwegingen moeten in aanmerking worden genomen:

- Naarmate de omvang van de gecompromitteerde gegevens toeneemt wordt het een aantrekkelijker instrument voor misbruik en wordt de kans dat de betrokkenen last hebben van het lek groter. Dit geldt vooral voor databanken van de overheid.
- Naarmate de gecompromitteerde gegevens worden gebruikt om ingrijpender beslissingen te nemen over de betrokkene wordt ook de impact groter. Als een hacker bijvoorbeeld toegang heeft tot gegevens in een databank en deze kan wijzigen, welke gegevens gebruikt worden om iemands kredietwaardigheid te bepalen, zijn de gevolgen ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.
- Als de gecompromitteerde gegevens worden gebruikt door een keten van instanties heen – wat vaak het geval is bij overheden en zorgverleners – wordt het moeilijker om de gevolgen van een verlies of wijziging van gegevens te beheersen, en wordt de impact van het lek groter.
- Indien de gegevens specifiek betrekking hebben op kwetsbare groepen, zoals kinderen, of personen die minder goed met computers overweg kunnen, wordt het moeilijker voor de

betrokkenen om de gevolgen van het incident te beheersen en is daarom de impact van het lek waarschijnlijk groter.
- Bepaalde incidenten brengen een hoger risico op misbruik met zich mee, bijvoorbeeld een hack.

Hoe en wanneer moet de melding aan het CBP worden gedaan?
- Meldingen aan het CBP kunnen via een webformulier of fax worden gedaan.
- De melding dient plaats te vinden op de tweede werkdag na ontdekking van het incident door de verantwoordelijke of diens verwerker. (Het incident moet bijvoorbeeld uiterlijk op dinsdag worden gemeld als het op vrijdag ontdekt werd).
- Het is mogelijk om de melding te wijzigen of aan te vullen of zelfs achteraf in te trekken.

4. Melden aan de betrokkene

Indien de verantwoordelijke op basis van het bovenstaande een melding aan het CBP moet doen is de volgende vraag of hij ook een melding aan de betrokkene moet doen. De relevante overweging is of het incident waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene(n).

Heeft de verantwoordelijke voldoende maatregelen voor gegevensbescherming genomen om de melding aan de betrokkene achterwege te kunnen laten?

Indien de verantwoordelijke beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegde derden kan hij de melding aan de betrokkene achterwege laten. Het CBP noemt de volgende maatregelen als voorbeelden:

- *Versleuteling*
- *Remote wipe.* De verantwoordelijke moet vaststellen of de *remote wipe* tijdig in gang is gezet, of het apparaat nog een *remote wipe* instructie kon ontvangen en uitvoeren, en of de *remote wipe* elke mogelijkheid tot reconstructie van de gegevens voorkomt.
- *Pseudonimisering.* Deze maatregel moet het opnieuw identificeren van de betrokkene effectief voorkomen.

Voor wat betreft versleuteling:
- Indien de persoonsgegevens vernietigd zijn zal versleuteling geen schade aan de betrokkene voorkomen. In dat geval kan alsnog van een verantwoordelijke gevraagd worden om de betrokkene op de hoogte te stellen.
- De versleuteling moet actief zijn geweest op het moment van het incident.

- De versleuteling moet gebaseerd zijn op een standaardalgoritme (bijvoorbeeld als gepubliceerd door het EU Agency for Network and Information Security, ENISA).
- Het algoritme kan worden beschouwd als voldoende veilig voor de toekomst indien het is gekwalificeerd als geschikt voor 'future use' (toekomst-vast voor de komende 10 tot 50 jaar) door ENISA.
- De verantwoordelijke moet rekening houden met eventueel gepubliceerde kwetsbaarheden in het algoritme.
- De implementatie van het versleutelingsalgoritme dient voldoende veilig te zijn. Dit moet eventueel worden vastgesteld door een (externe) deskundige.
- De beveiliging moet geheim blijven en mag bijvoorbeeld niet gelekt zijn in het kader van het incident.

Tenslotte moet de verantwoordelijke vaststellen of – in het licht van alle toepasselijke veiligheidsmaatregelen – er nog steeds een risico op onbevoegde verwerking van de persoonsgegevens bestaat, nu *of in de toekomst.*

Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene?
Indien we ervan uitgaan dat de beveiligingsmaatregelen onvoldoende waren zal de verantwoordelijke moeten bepalen of er waarschijnlijk ongunstige gevolgen zullen zijn voor de persoonlijke levenssfeer van de betrokkene. Indien het datalek gevoelige gegevens omvat (zoals hierboven gedefinieerd) moet de verantwoordelijke een melding doen aan de betrokkene. In andere gevallen zal de verantwoordelijke moeten afwegen wat de waarschijnlijke ongunstige gevolgen voor de betrokkene zullen zijn en of hij informatie moet krijgen over het datalek om zichzelf tegen die ongunstige gevolgen te beschermen.

Zijn er dringende omstandigheden waardoor het (vooralsnog) niet aan te raden is een melding te doen aan betrokkene?
De verantwoordelijke kan ertoe besluiten om de melding aan betrokkene uit te stellen of helemaal niet te doen in situaties waarin dit een noodzakelijke maatregel is in het belang van:

- de voorkoming, opsporing en vervolging van strafbare feiten;
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de bovenstaande twee belangen;
- de nationale veiligheid;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen (inclusief de verantwoordelijke).

Voorbeelden van belangen in de laatste categorie zijn:

- Wanneer gegevens van een kind dat vertrouwelijk om hulp heeft gevraagd bij huiselijk geweld betrokken zijn geraakt in een datalek kan de verantwoordelijke besluiten om geen melding te doen aan de betrokkene uit angst dat zijn ouders er dan achter komen.
- De belangen van de verantwoordelijke worden zo disproportioneel aangetast dat hij in zijn rechten en vrijheden wordt aangetast. Als de verantwoordelijke bijvoorbeeld op het punt staat een overname van/door een ander bedrijf te voltooien en er zich een datalek voordoet mag hij de melding aan de betrokkene uitstellen (maar niet de melding aan het CBP).

Hoe en wanneer moet de melding aan de betrokkene worden gedaan?
De betrokkene moet onverwijld op de hoogte worden gesteld. Dit betekent dat de verantwoordelijke:

- enige tijd mag nemen voor nader onderzoek om een behoorlijke en zorgvuldige melding voor te bereiden.
- er rekening mee moet houden dat de betrokkene mogelijk maatregelen moet nemen om zich te beschermen tegen schade.
- een eerste melding mag doen om betrokkenen in de gelegenheid te stellen bijvoorbeeld hun wachtwoorden te veranderen, zonder (nog) de volledige details te geven.

De verantwoordelijke zal aan het CBP moeten melden wanneer hij van plan is de melding aan de betrokkene te doen. Deze toezegging is bindend voor de verantwoordelijke, tenzij hij de melding later aanpast.

5. Na de melding
Een overzicht van het incident bewaren
De verantwoordelijke moet een overzicht bewaren van alle datalekken die ernstig genoeg waren om melding aan het CBP te doen. Dit overzicht hoeft niet openbaar te worden gemaakt.

Elk overzicht moet minimaal één jaar na de definitieve melding aan de betrokkene worden bewaard. In het geval de verantwoordelijke besloten had de betrokkene niet te informeren (bijvoorbeeld vanwege versleuteling of een doorslaggevend dringend belang waardoor dit niet kan) moeten de gegevens ten minste drie jaar worden bewaard. In dat geval moet de melding ten minste eenmaal per jaar worden geëvalueerd of er na enige tijd redenen zijn om alsnog te melden (bijvoorbeeld wanneer de versleuteling een kwetsbaarheid blijkt te bevatten).

Hoe reageert het CBP bij ontvangst van een melding?
Als de melding het CBP aanleiding geeft tot nadere actie, dan zal het CBP daarover contact met de verantwoordelijke opnemen.

- In eerste instantie zal het daarbij gaan om verificatie dat de gedane melding daadwerkelijk van de verantwoordelijke afkomstig is, en om eventuele inhoudelijke vragen over de melding.
- Als de verantwoordelijke ten onrechte heeft besloten om betrokkenen niet te informeren kan het CBP van de verantwoordelijke verlangen dat hij betrokkenen alsnog informeert.
- Het CBP houdt een niet-openbaar register bij van alle ontvangen meldingen.
- Alleen als de verantwoordelijke een apert onredelijke interpretatieruimte heeft toegepast (door de melding over het incident achterwege te laten) zal het CBP een boete opleggen.

Kennedy Van der Laan

Contact

Maarten Goudsmit
020 - 5506 683
maarten.goudsmit@kvdl.com

Maarten Goudsmit is medewerker van de Teams Privacy en Informatietechnologie en werkt sinds 2012 bij Kennedy Van der Laan. In 2004 begon Maarten aan zijn studie rechten aan de Universiteit van Amsterdam en studeerde af met een specialisatie in informatierecht. Na het behalen van zijn masterstitel in Amsterdam studeerde Maarten IP & IT Law aan de Fordham University in New York City, en behaalde daar zijn LL.M magna cum laude. Voordat hij naar Kennedy Van der Laan overstapte werkte Maarten anderhalf jaar als advocaat bij een ander groot advocatenkantoor in Amsterdam.