Postbus 21695
3001 AR Rotterdam
F: 010 201 35 01
E: secretariaat@verenigingprivacyrecht.nl
ABN AMRO NL50ABNA0607516771
KvK Rotterdam 34335879
www.verenigingprivacyrecht.nl

Aan: College bescherming persoonsgegevens
Datum: 15 oktober 2015
Betreft: Consultatie richtsnoeren datalekken

Op woensdag 14 oktober 2015 vond het PrivacyDebat van de Vereniging Privacy Recht plaats over de consultatieversie van de richtsnoeren meldplicht datalekken. Gezien de beperkte tijd voor een reactie op de consultatieversie is ervoor gekozen om de diverse punten die tijdens het debat aan de orde zijn gekomen schriftelijk samen te vatten. Deze standpunten geven een goed beeld van de binnen de vereniging aanwezige gedachten en meningen, die overigens breed gedragen werden door de aanwezigen.

Het debat werd ingeleid door prof. mr. Gerrit-Jan Zwenne (Universiteit Leiden/ Bird & Bird) en mr. Jan A.N. Baas (BarentsKrans). Moderator was mr. Huib J.M. Gardeniers (Net2Legal Consultants). Notulist was mr. Roderick J. Watson (BarentsKrans).

Status richtsnoeren

- Aannemelijk is dat de richtsnoeren moeten worden aangemerkt als beleidsregel zoals bedoeld in artikel 1:3 lid 4 Awb. Indien het CBP dit standpunt deelt zou het goed zijn als dat expliciet in de richtsnoeren wordt vermeld.

Definitie 'datalek'

- Terminologie wordt door het document heen niet consequent toegepast. In het bijzonder wordt gewezen op passages:
  - op pagina 15: "*Een datalek wordt in de Wbp gedefinieerd als "een inbreuk op de beveiliging, bedoeld in artikel 13 (artikel 34a lid 1 Wbp) Kortheidshalve wordt een dergelijke inbreuk in deze richtsnoeren aangeduid als een datalek*"
  - en pagina 17: "*dan is er uitsluitend sprake van een beveiligingslek en niet van een datalek*".

  De passage op pagina 15 lijkt onjuist, omdat een definitie van "datalek" niet in de wet is opgenomen. Een datalek impliceert daarnaast dat er tenminste gegevens verloren zijn gegaan of onrechtmatig verwerkt. Dat element ontbreekt in de voorgestelde definitie.
- Het lijkt beter om consequent te spreken van beveiligingsinbreuk (*security breach*) voor het geval dat er een inbreuk is gemaakt op de beveiliging en van een datalek (*personal data breach*) indien er tevens gegevens verloren zijn gegaan of onrechtmatig verwerkt.
- Meer principieel is echter opgemerkt dat de term 'datalek' hoe dan ook onduidelijk en verwarrend is omdat deze term in het spraakgebruik een veel beperktere lading heeft dan er door het CBP aan wordt toegekend ("lek" impliceert dat er bijvoorbeeld gegevens in verkeerde handen zijn geraakt, de link naar "verloren gaan" van gegevens zal minder snel worden gelegd). Dat zou een argument zijn om geheel bij deze term weg te blijven.

Onjuist of tenminste verwarrend gebruik van het begrip 'bestand'

- In een voorbeeld op pagina 20 wordt gerefereerd aan een enveloppe met creditcard betalingsgegevens van 800 personen. Een dergelijke enveloppe valt niet noodzakelijkerwijze onder de wet (definitie bestand in artikel 1, onder c Wbp); dat is pas het geval indien de gegevens gestructureerd zijn en volgens bepaalde criteria toegankelijk. Dit voorbeeld dient verduidelijkt te worden of te vervallen.

Positie bewerker

- De tekst op pagina 13: "*Hoewel u als verantwoordelijke verantwoordelijk en aansprakelijk bent voor de gegevensverwerking door de bewerker (zie art. 12 Wbp), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens die zijn opgenomen in hoofdstuk 1 en 2 van de Wbp*"

  Deze passage roept vragen op. Is het juist dat het hier (louter) gaat om de civielrechtelijke aansprakelijkheid? De tekst is volgens de aanwezigen in dit opzicht niet duidelijk.

Te ruime lezing "inbreuk op de beveiliging" en "ernstig nadelige gevolgen"

- De wetgever heeft van meet af aan een clausulering van de meldplicht beoogd, gelet op de ruime werking van de Wbp (vgl. Kamerstukken II 2013/2014, 33 662, nr. 7, p. 5). Deze clausulering blijkt niet uit de conceptrichtsnoeren, die veelal kiezen voor een verruimende lezing. Ook zijn voorbeelden uit de parlementaire geschiedenis weggelaten die de meldplicht inperken.
- Op pagina 16 wordt in dit verband ten onrechte verlies van persoonsgegevens, ontstaan als gevolg van een calamiteit zoals een blikseminslag die een brand veroorzaakt, gezien als een verlies van persoonsgegevens, veroorzaakt door een beveiligingsinbreuk. Ditzelfde geldt voor het verloren gaan van een database door een menselijke fout. Deze voorbeelden worden in de parlementaire geschiedenis juist expliciet uitgesloten.
- De voorbeelden in de richtsnoeren zien op grote aantallen betrokkenen (zie p. 30, 1000 betrokkenen, en pagina 34 met voorbeelden over 2000 of 700 betrokkenen. Hoe pakken deze voorbeelden uit bij (aanzienlijk) kleinere aantallen?
- De parlementaire geschiedenis geeft een aantal overige voorbeelden van situaties die niet gemeld hoeven te worden, zoals het hacken van de ledenadministratie van een sportvereniging (MvT, p. 7) en de hack van een gemeentelijke website voor een gratis jeugdsportpas. Hoe kijkt het CBP tegen dit soort voorbeelden aan?
- De tekst op pagina 16 over malware is erg algemeen gesteld. Als wordt bedacht hoeveel besmettingen er plaats vinden met malware, en hoe verschillend de betreffende types malware zijn, leidt deze tekst, die uitgaat van melden in (bijna) alle gevallen van malwarebestemming, tot een te ruime en ongedifferentieerde meldplicht.

- Daarnaast werd de vraag gesteld of bijvoorbeeld een vertraagde update van een beveiligingspakket moet leiden tot een melding, en bijvoorbeeld hoe lang de verminderde beveiliging moet hebben geduurd voordat er een melding zou moeten worden gedaan. Het zal in die situaties niet duidelijk zijn of er daadwerkelijk sprake is geweest van een datalek.

Termijn waarbinnen de melding aan het CBP moet worden gedaan ('onverwijld')

- De termijn van twee werkdagen om een datalek te melden geeft aanleiding tot veel discussie. Aanwezigen wijzen op het feit dat deze termijn onder omstandigheden (soort verantwoordelijke, betrokkenheid meer partijen zoals bewerkers) te kort kan zijn. Deze twee werkdagen geven immers geen ruimte om te onderzoeken of daadwerkelijk sprake is van een datalek en of deze meldingsplichtig is onder de Wbp. De aanwezigen vrezen dat deze situatie veel bedrijven dwingt om dan maar voor de zekerheid te melden wat voor alle partijen onnodig werk meeneemt (pro forma meldingen).
- Er zijn echter ook aanwezigen die erop wijzen dat in specifieke gevallen zoals bij een ernstig lek, twee werkdagen een lange termijn kan zijn omdat deze ertoe kan leiden dat het Cbp pas in een betrekkelijk laat stadium van een ernstig lek op de hoogte wordt gesteld. Zeker als het lek toevallig zou plaatsvinden in een weekend dat wordt gevolgd door feestdagen.
- De vraag is of de termijn van twee werkdagen niet veeleer als een vuistregel gehanteerd zou dienen te worden waarbij, afhankelijk van de omstandigheden, ook een snellere melding geïndiceerd kan zijn, of juist meer tijd genomen kan worden.
- In dit verband werd overigens ook opgemerkt dat het melden van het datalek binnen twee werkdagen niet altijd betekent dat de schade kleiner wordt, zeker als er al veel tijd tussen ontstaan en ontdekking van het datalek is verstreken. Vervolgens is het ook de vraag hoe snel het CBP iets met een melding zal doen.
- Er zijn aanwezigen die zich afvragen waarom niet is aangesloten bij een internationale standaard van het doen van een melding binnen 72 uur.
- Ook werd geopperd aan te sluiten bij de wijze waarin in het arbeidsrecht wordt omgegaan met ontslag op staande voet. Daarbij geldt dat er eerst met voortvarendheid onderzoek moet worden gedaan. Als de uitkomsten van het onderzoek daartoe aanleiding geven, moet er vervolgens onverwijld worden overgegaan tot ontslag op staande voet. Een dergelijk systeem zou ook in het leven kunnen worden geroepen voor het melden van datalekken.
- Als er met een open norm zou worden gewerkt, dan zou het Cbp wel moeten aangeven welke omstandigheden bepalen hoe lang die termijn is. De lengte van de termijn zou bijvoorbeeld afhankelijk kunnen worden gemaakt van de gevoeligheid van de gegevens en de complexiteit van het datalek, waarbij de verschillende criteria eventueel in een tabel zouden kunnen worden weergegeven.

Wanneer vangt de termijn aan waarbinnen de melding moet worden gedaan

- Het is niet voor iedereen duidelijk wat het moment van ontdekking van het datalek is. Dat is relevant omdat de meldtermijn gaat lopen op het moment van ontdekking. Van een 'datalek' is immers pas sprake indien vastgesteld is dat persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking en dat niet uitgesloten kan worden dat gegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Er wordt tevens geopperd dat de meldingstermijn pas dient aan te vangen zodra het de verantwoordelijke bekend is dat er sprake is van een *meldingsplichtig* datalek.

Bewaartermijn van één jaar in hoofdstuk 10 van de richtsnoeren

- Het is de vraag wat nog de ratio is van deze verplichting, nu de verplichting alleen nog maar ziet op datalekken die onder de meldplicht vallen (vgl. brief CBP 20 februari 2014).
- Vanuit een goed beveiligingsbeleid zou het veeleer in de rede liggen dit soort informatie lang te bewaren, om incidenten die zich voordoen in verband te kunnen brengen met incidenten die zich in het verleden hebben voorgedaan en om lering te kunnen (blijven) trekken uit incidenten uit het verleden.

Misbruik

- De vraag is opgekomen of er een voorziening zou moeten worden getroffen om misbruik (valse meldingen) te voorkomen. Op de manier waarop het nu geregeld is kan een ieder een melding doen en zich bijvoorbeeld voordoen als iemand anders.

Toekomstbestendigheid richtsnoeren

- Er wordt gevraagd hoe toekomstbestendig de richtsnoeren nu eigenlijk zijn. Dit in het licht van het feit dat er al in 2017 een evaluatie van de richtsnoeren zal volgen en op enig moment de Algemene Verordening Gegevensbescherming van kracht zal worden. Vanuit het oogpunt van kosten en werkzaamheden verbonden aan de implementatie van regels en beleid werd aangegeven dat het onwenselijk is om de praktijk te confronteren met teveel wijzigingen van de regels en beleid.

Meldplicht financiële instellingen

- Diverse aanwezigen waren van mening dat de toelichting op de uitzondering voor financiële ondernemingen zoals bedoeld in de Wft en de samenhang met de meldplicht voor de telecomsector, zoals bij samenloop, erg summier was.

Meldplicht ten aanzien van gepseudonimiseerd bestand

- De vraag werd gesteld in hoeverre het lek van een 'gepseudonimiseerd' bestand een meldplicht in het leven roept. En in hoeverre heeft de stand van de techniek, en dus de mogelijkheid om bestanden te de-pseudonimiseren, hier invloed op? De tekst roept vragen op. Er werd zelfs geopperd om de passage over gelekte gegevens die gepseudonomiseerd zijn uit de richtsnoeren te verwijderen.

Meldplicht bij het CBP ten aanzien van bestand dat 'geëncrypt' is, of dat van andere technische beschermingsmaatregelen is voorzien.

- Artikel 34a lid 6 maakt duidelijk dat de verplichting om de betrokkene te informeren niet van toepassing is ingeval van (effectieve) technische beschermingsmaatregelen. Maar hoe zit dit ten aanzien van de verplichting om te melden bij het CBP? Tenminste één voorbeeld op pagina 20 suggereert dat in het geval van deugdelijke encryptie, ook niet gemeld hoeft te worden bij het CBP (er is dan geen kans op nadelige gevolgen voor de bescherming van persoonsgegevens). Het zou wenselijk zijn dat het CBP expliciet aangeeft of de meldplicht in een dergelijk geval wel of niet aan de orde is.

Opmerkingen van algemene aard

Gevoelige persoonsgegevens

- De richtsnoeren besteden nadrukkelijk aandacht aan 'gevoelige persoonsgegevens'. Hiermee lijkt een nieuwe categorie gegevens te ontstaan naast de 'bijzondere persoonsgegevens'. Het is onduidelijk wat de consequenties van deze nieuw benoemde groep gegevens voor andere vraagstukken dan datalekken is. Ten onrechte wordt de suggestie gewekt dat deze 'gevoelige persoonsgegevens' een soort 'bijzondere persoonsgegevens' zijn, of dat in elk geval een nieuw type persoonsgegevens wordt ingevoerd welke aparte behandeling behoeven.

Transparantie rond consultatie door het CBP

- Bij consultatie over beleid-, wet- en regelgeving is transparantie vereist. Daarbij past niet dat consultatieversies van richtsnoeren (zoals recent die m.b.t. cameratoezicht en thans met de meldplicht datalekken en de boeterichtsnoeren) vertrouwelijk en onder embargo aan door het college zelf geselecteerde stakeholders en deskundigen worden verstrekt. Daarnaast zou het plezierig zijn indien het CBP, gelet op de genomen moeite om tot reacties te komen, op de zienswijzen reageert en aangeeft in hoeverre, en om welke redenen, aangedragen punten wel of niet hebben geleid tot aanpassing.

VPR/oktober 2015