Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31(0)6 3964 2738
E rejo.zenger@bof.nl
W www.bof.nl

Bank account 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

Ministerie van Veiligheid en Justitie

Betreft
Inbreng consultatie meldplicht datalekken

Datum
Amsterdam, 29 februari 2012

Geachte heer, mevrouw,

1. Graag reageert stichting Bits of Freedom op het wetsvoorstel voor een meldplicht datalekken.

   Bits of Freedom is zeer verheugd dat het ministerie dit wetsvoorstel heeft gepubliceerd. De vele datalekken in de laatste twee jaar onderstrepen de noodzaak van zo'n meldplicht.[1] We zijn blij dat het ministerie deze noodzaak onderstreept door in het voorstel een maximumboete van 200.000 euro op te nemen. We zien ook dat het ministerie moeite heeft gedaan om de belangen van de betrokkene te behartigen.

2. In deze brief benadrukt Bits of Freedom dat het belangrijkste doel van zo'n meldplicht is: het beschermen van de betrokkene tot wiens gegevens onbevoegde toegang is verkregen en het verkrijgen van inzicht in de aard en omvang van de problematiek. Bits of Freedom komt tot de conclusie dat onder het huidige voorstel i) niet alle meldenswaardige datalekken gemeld hoeven te worden, ii) de betrokkene onvoldoende wordt geïnformeerd en iii) het register bij het College anderen niet in staat stelt om onderzoek te doen naar de aard en de omvang van de problematiek. Bits of Freedom zal dat in deze brief nader toelichten.

3. Bits of Freedom zal eerst het doel van zo'n meldplicht bespreken. Vervolgens wordt ingegaan op het uitgangspunt dat voor het wetsartikel moet gelden. Daarna worden alle belangrijke elementen van een effectieve meldplicht besproken. Tenslotte geeft Bits of Freedom aan hoe de adviezen het beste in het voorgestelde artikel kunnen worden verwerkt.

1 https://www.bof.nl/category/zwartboek-datalekken/

Doel meldplicht is bescherming betrokkene en verkrijgen inzicht

4. Er is sprake van een datalek op het moment dat onbevoegde toegang tot persoonsgegevens, die aan een verantwoordelijke zijn toevertrouwd, is verkregen. Dat is de kern van het probleem. Dit wordt verderop nader toegelicht. De gevolgen van een datalek voor een betrokkene kunnen verstrekkend zijn, waaronder de onthulling van de identiteit van iemand en identiteitsfraude.

   Voorbeeld: Samarium is een platform gericht op jongeren met sadomasochistische gevoelens. Via een forum op de website kunnen zij hun gevoelens met leeftijdsgenoten delen, zonder daarbij hun eigen identiteit kenbaar te maken. In deze anonieme wereld voelen de leden zich vrij om te praten. Toen de beheerders van de website bij de verzending van een e-mail een fout maakten, werden elkaars contact - gegevens bekend. Hierdoor is de identiteit van de betrokkenen bekend geworden bij de andere ontvangers. Als gevolg hiervan kunnen leden niet langer in alle vrijheid met elkaar praten. [2]

   Voorbeeld: Toen T-Mobile een klant probeerde te helpen met het inloggen op zijn persoonlijke pagina, worden de gebruikersnaam en het wachtwoord per ongeluk in een publiek bericht op Twitter gepubliceerd.[3] Snel daarna bleken derden direct zijn facturen te hebben ingezien en zijn abonnement te hebben aangepast.[4]

5. Het doel van een meldplicht is betrokkenen in staat te stellen om bij een datalek zo snel als mogelijk maatregelen te nemen om verdere schade te voorkomen. Ook dit wordt verderop nader toegelicht.

6. Een meldplicht zorgt ook voor bewustwording onder zowel betrokkenen en verantwoordelijken over de risico's die met de grootschalige verwerking van persoonsgegevens samenhangen. Dat zal er aan bijdragen dat een verantwoordelijke niet meer persoonsgegevens verwerkt dan strikt noodzakelijk is. Dat betekent ook dat een verantwoordelijke er voor zal zorgen gegevens te verwijderen indien deze niet meer nodig zijn. Een meldplicht is daar bovenop een stimulans om de verwerkte gegevens afdoende te beschermen. Tenslotte zal een publiek centraal register inzicht geven in de aard en omvang van het probleem. Dat stelt het bedrijfsleven en de overheid in staat beleid op het gebied van de bescherming van persoonsgegevens te maken dat gebaseerd is op feiten.

   Voorbeeld: Via de Nationale Theaterkassa worden toegangskaarten voor concerten en theater verkocht. Sinds 2010 is de website overgestapt op een nieuw systeem voor het verwerken van de aankopen. De oude databank bleef alleen nog maar in gebruik voor de verzending van de nieuwsbrief. Na een datalek bleek deze databank niet alleen nog maar e-mailadressen te bevatten, maar ook de gegevens van 2.100 creditcards, waarvan er nog 226 actief zijn. Deze gegevens waren, tegen de regels van de verstrekkers van de creditcards in, niet versleuteld opgeslagen en konden door onverlaten worden misbruikt. Zodra de eigenaren van deze creditcards op de hoogte worden gesteld, kunnen zij

2 https://www.bof.nl/2011/08/01/mailen-is-moeilijk-juli-2011/
3 https://www.bof.nl/2010/09/18/datalek-t-mobile-tweet-inloggegevens-klant/
4 http://twitter.com/#!/MarkSedney/status/24753362472

maatregelen nemen om misbruik te voorkomen.[5]

Voorbeeld: Nadat de omroep Llink werd opgeheven, werd de website vergeten. Deze blijkt lek te zijn en de databank met de gegevens van 153.000 leden kwamen op straat te liggen. Hoewel Llink inmiddels is opgeheven, zijn dit soort omvangrijke lekken een belangrijk gegeven voor beleidsmakers. Het is dus goed als dit soort lekken in een centraal register worden bijgehouden.[6]

Elk lek moet worden gemeld, ook bij afwezigheid van beveiligingsmaatregelen

7. Onder onbevoegde toegang wordt verstaan elke onbevoegde kennisneming van persoonsgegevens. Hieronder valt élke onbevoegde kennisneming van persoonsgegevens, zowel binnen als buiten de organisatie van de verantwoordelijke. Deze term dient ruim te worden uitgelegd. Naast het onbevoegde kennisnemen valt in ieder geval ook het onbevoegde kopiëren hieronder.

   Voorbeeld: Uit een uitspraak van een rechter blijkt dat een secretaresse van een gezondheidsinstelling haar toegang tot het Elektronisch Patiënten Dossier (EPD) heeft misbruikt voor privé doeleinden. Nadat een dochter van de vrouw was aangerand, werd van aangifte afgezien op voorwaarde dat de man zich zou laten behandelen. De vrouw controleerde de status van de behandeling in het EPD, ook al was zij daartoe niet bevoegd. Dit is een vorm van onbevoegde kennisneming die als datalek zou moeten worden aangemerkt.[7]

   Voorbeeld: Opsporings- en inlichtingendiensten vragen regelmatig de zogenaamde verkeersgegevens van klanten van aanbieders van mobiele telefonie op. Verkeersgegevens zeggen iets over wie met wie en wanneer contact heeft gehad, maar niets over de inhoud van de communicatie. In 2009 werd duidelijk dat Vodafone en T-Mobile ten onrechte ook de inhoud van de sms-berichten met de opsporings- en inlichtingendiensten deelden. De opsporings- en inlichtingendiensten namen de inhoud van de berichten ook over in hun systemen en dossiers. De diensten hadden geen bevoegdheid voor het lezen van de inhoud van de berichten en daarmee is sprake van onbevoegde toegang. Ook dit zou als datalek moeten worden aangemerkt.[8]

   Voorbeeld: In oktober bleek een online winkel voor baby-artikelen onvoldoende beveiligd. Eerder deze maand werden de gegevens van 539 accounts gepubliceerd. Deze publicatie werd ingegeven door een ander datalek en betrof een specifieke selectie van klanten.[9] Het is aannemelijk dat de aanvallers de volledige databank van 134.000 gebruikers hebben gekopieerd en niet slechts de 539 gepubliceerde accounts.[10] Het is niet duidelijk of er, in strikte zin, sprake is van kennisname van álle gegevens. Nu deze gegevens in ieder geval zijn gekopieerd, moet dit ook als datalek worden aangemerkt.

8. Ook als er sprake is van onbevoegde toegang zonder dat beveiligingsmaatregelen worden doorbroken kan dit gevolgen voor de betrokkene hebben.

   Voorbeeld: Met de Rabobank E-Scan kunnen mensen hun geschiktheid als ondernemer onderzoeken.

5 https://www.bof.nl/2012/02/23/datalek-nationale-theaterkassa-lekt-creditcardgegevens/
6 https://www.bof.nl/2011/06/16/datalek-gapend-gat-in-databank-opgeheven-omroep-2/
7 https://www.bof.nl/2010/09/24/datalek-secretaresse-raadpleegt-epd-voor-privedoeleinden/
8 http://vorige.nrc.nl/binnenland/article2256668.ece/Smsjes_gaan_ongevraagd_naar_politie
9 https://www.bof.nl/2012/02/17/datalek-gegevens-klanten-baby-dump-op-straat/
10 http://www.nrc.nl/nieuws/2012/02/11/opta-gaat-onderzoeken-of-kpn-klantgegevens-wel-goed-beschermde/

Aan de hand van meer dan honderd vragen, waarin ook iemands psychologische eigenschappen aan bod komen, stelt de bank een persoonlijk profiel op. Het rapport is via de website van de Rabobank te downloaden. Door het aanpassen van een cijfer in het adres van de pagina op de website, waren echter de rapporten van 3.300 anderen te raadplegen. En hoewel de profielen zeer persoonlijke informatie bevatten, leken op het eerste gezicht geen beveiligingsmaatregelen te zijn genomen. [11] Dat betekent dat dit niet als datalek zou worden aangemerkt in het concept-wetsvoorstel van het ministerie: een duidelijk ongewenste uitkomst.

Voorbeeld: Kasboek.nl geeft gebruikers de mogelijkheid om via de website hun persoonlijke financiën inzichtelijk te maken. Gebruikers sturen daarvoor een kopieën van hun digitale rekeningafschriften naar de website. De beheerders plaatsen de afschriften in een publiek toegankelijke en niet-beveiligde directory op de server. Meer dan een miljoen transacties met een totale waarde van ongeveer 200 miljoen euro waren in te zien. Uit de omschrijvingen bleek dat er 3.362 keer salaris werd uitbetaald, in 5.332 gevallen geld van of naar de Belastingdienst werd overgemaakt, 147 mensen alimentatie betaalden en één betrokkene 1.459 euro aan een winkel met erotische artikelen overmaakte. [12] Omdat deze gegevens vrij toegankelijk waren op internet, zou ook dit in het concept-wetsvoorstel van het ministerie niet als datalek worden aangemerkt. Ook dat is een duidelijk ongewenste uitkomst.

9. Zodra onbevoegde toegang is verkregen tot persoonsgegevens moet de betrokkene worden geïnformeerd. Immers: onbevoegde toegang is het probleem (zie paragraaf 2) en de meldplicht is er om de schade voor de betrokkene te beperken (zie paragraaf 3). Het is daarom essentieel dat “onbevoegde toegang” als uitgangspunt voor het wetsartikel wordt gebruikt. In het huidige voorstel is dat niet het geval, want daar wordt uitgegaan van “een inbreuk op de maatregelen als bedoeld in artikel 13”.

10. Onbevoegde toegang tot persoonsgegevens als uitgangspunt voor het wetsartikel kent drie belangrijke voordelen:

    - De betrokkene wordt altijd geïnformeerd bij toegang tot zijn persoonsgegevens waaraan (in de meeste gevallen negatieve) consequenties voor de betrokkene zijn verbonden. Onder het huidige voorstel hoeft de verantwoordelijke onbevoegde toegang tot persoonsgegevens niet aan de betrokkene melden als niet ook sprake is van een inbreuk op de maatregelen als bedoeld in artikel 13. Dit wordt bevestigt in de Toelichting, op pagina 8. Dat is zeer problematisch. Uit het Zwartboek Datalekken blijkt dat lang niet altijd passende beveiligingsmaatregelen zijn genomen, zodat bepaalde datalekken dus niet gemeld zouden hoeven te worden.

    - De administratieve lasten voor de verantwoordelijke en het College nemen af omdat incidenten die niet hebben geleid tot onbevoegde toegang tot persoonsgegevens niet hoeven te worden gemeld. In het huidige voorstel geldt dat als is voldaan aan de voorwaarden van het eerste lid, maar de persoonsgegevens niet leesbaar zijn, het incident toch gemeld moet worden bij het College. Door onbevoegde toegang als

11 https://www.bof.nl/2012/01/31/datalek-rabobank-lekt-duizenden-ondernemersrapporten/
12 https://www.bof.nl/2010/10/07/datalek-miljoenen-transacties-van-online-huishoudboek/

uitgangspunt te nemen hoeven lekken van versleutelde informatie niet meer te worden gemeld.

- Het College wordt verder ontlast omdat er geen directe opvolging op de melding door een verantwoordelijke nodig is. In het huidige voorstel moet het College beoordelen of het beroep op lid 6 door de verantwoordelijke terecht is. Deze beoordeling moet direct na de melding gebeuren. Dat is nodig omdat uitstel van de melding aan de betrokkene betekent dat de betrokkene zich minder goed kan beschermen tegen de gevolgen van het lek. Dit wordt nader toegelicht in paragraaf 19.

Elk lek moet gemeld worden, ook indien dat slechts vermoed moet worden

11. Ook bij een vermoeden dat er sprake is van onbevoegde toegang moet de betrokkene hierover worden geïnformeerd.

> Voorbeeld: Twee weken geleden is een rechercheur van de politie Rotterdam-Rijnmond een dossier met informatie over een opsporingsonderzoek verloren. Het dossier bevatte kopieën van verhoren, foto's en persoonlijke informatie van verdachten. De rechercheur had het dossier bij vertrek op het dak van haar auto laten liggen. Een groot aantal medewerkers van de politie heeft het dossier gezocht, maar zonder resultaat.[13] De verantwoordelijke vermoedt in zo'n situatie dat er sprake is van onbevoegde toegang en de betrokkene zou over dit datalek moeten worden geïnformeerd.

Elk lek moet gemeld worden, ongeacht gevolgen voor betrokkene

12. Naar de mening van Bits of Freedom zouden de gevolgen voor de betrokkene van een datalek niet relevant horen te zijn voor de vraag of dit lek gemeld moet worden. In het huidige voorstel hoeft er geen melding aan het College en de betrokkene gedaan worden als niet “redelijkerwijs aangenomen kan worden is dat de inbreuk nadelige gevolgen voor [de betrokkene]” heeft. De verantwoordelijke, noch het College, is echter in staat de gevolgen voor de betrokkene goed in te schatten.

> Voorbeeld: Begin dit jaar lekte een Udense Vuurwerkhandel de gegevens van ruim 9.000 orders. In de orders staan onder meer adressen en telefoonnummers van klanten. De verantwoordelijke zou kunnen betogen dat het niet redelijkerwijs aangenomen kan worden dat dit lek nadelige gevolgen voor de betrokkene heeft. Een betrokkene die, om welke reden dan ook, niet kenbaar heeft willen maken dat hij vuurwerk gekocht heeft, ondervindt van dit lek echter wel nadelige gevolgen. Hetzelfde geldt voor de betrokkene die, om welke reden ook, zijn woon- of e-mailadres geheim wil houden.

Melding aan betrokkene moet altijd geïnformeerd worden, ongeacht andere meldplichten

13. De betrokkene moet altijd geïnformeerd worden, ook als op de verantwoordelijke een meldplicht op grond van bijvoorbeeld de Wet op het financieel toezicht of de Telecommunicatiewet rust. Als

13 http://www.politiepersberichten.nl/rotterdam-rijnmond-zuid-holland-zuid/bericht/29788/

de toets van zo'n meldplicht melding aan de betrokkene niet afdwingt, dan moet dat alsnog gebeuren op grond van deze meldplicht.

Melding aan betrokkene moet volledig zijn

14. De betrokkene kan zich alleen goed beschermen tegen de gevolgen van een datalek als de melding volledig is. In de voorgestelde melding aan de betrokkene ontbreekt i) de aard van de gelekte informatie, ii) de mogelijke consequenties voor de betrokkene en iii) een beschrijving van de door de organisatie genomen stappen voor het inperken van de gevolgen voor de betrokkene. Dat is nodig omdat alleen op die manier de betrokkene goed kan beoordelen welke maatregelen hij zelf kan of moet nemen.

15. Het komt geregeld voor dat de betrokkene geen idee heeft dat zijn gegevens bij de verantwoordelijke bekend zijn en al helemaal niet welke gegevens dat zijn.

    Voorbeeld: Eerder deze maand bleek de website van Nobiles, een bedrijf dat carrièreadvies aan studenten geeft, onvoldoende beveiligd. De achterliggende databank, met gegevens van 338.000 accounts bleek hierdoor publiek toegankelijk. De gegevens van 900 accounts zijn op internet gepubliceerd.[14] In een reactie op een e-mail van Nobiles schrijft een van de betrokkene dat hij niet eens wist dat hij een account had.[15]

16. Alleen als de betrokkene een compleet en gedetailleerd overzicht van het soort gelekte gegevens heeft kan hij goed beoordelen welke maatregelen hij zelf kan of moet nemen. Als in de melding gesproken wordt over gegevens van creditcards, dan is daarmee nog niet duidelijk of dit het volledige creditcardnummer is of slechts de laatste vier cijfers. Evenmin is duidelijk of ook de SecureCode gelekt is. In de melding moet zo nauwkeurig als mogelijk vermeld worden welke gegevens in welke vorm gelekt zijn.

    Voorbeeld: Een website voor de verkoop van concertkaarten bleek bijzonder slecht beveiligd te zijn en lekt behalve vertrouwelijke bedrijfsinformatie ook de administratie van klantgegevens. Een beveiligings - onderzoeker had toegang tot onder meer creditcardnummers, die niet versleuteld zijn opgeslagen. De verantwoordelijke kan in zo een geval niet volstaan met de melding dat een datalek heeft plaats - gevonden. Als hij niet vermeldt dat ook onbevoegde toegang is verkregen tot de gegevens van creditcards, zal de betrokkene zich namelijk mogelijk niet realiseren dat het goed is om de creditcard te blokkeren. [16]

17. De betrokkene moet geïnformeerd worden over de geconstateerde en vermoedelijke gevolgen van het lek. Zo gebruiken veel mensen hetzelfde wachtwoord voor meerdere websites. Dat betekent dat als het wachtwoord via de ene website op straat komt te liggen, de betrokkene ook aangeraden moet worden het wachtwoord op andere websites aan te passen.

14 https://www.bof.nl/2012/02/22/datalek-300000-klantgegevens-carrieresite-toegankelijk/
15 https://twitter.com/#!/bvdhaterd/status/170503901437640706
16 https://www.bof.nl/2011/09/06/datalek-ticketsite-lekt-creditcardgegevens/

Voorbeeld: Het eerder genoemde Nobiles stuurde een e-mail aan haar gebruikers om hen te informeren over het gelekte wachtwoord. Nobiles geeft aan dat zij het wachtwoord al aangepast heeft om misbruik te voorkomen. Het bedrijf schrijft verder “Als je het wachtwoord voor Nobiles ook gebruikte op andere plekken (bijvoorbeeld Facebook, Hyves, Marktplaats etc.), dan adviseren wij je om dit ook te wijzigen.” [17] Dat is een goed advies.

18. Het is noodzakelijk dat de betrokkene op de hoogte wordt gebracht van de maatregelen die de verantwoordelijke reeds heeft genomen om gevolgen voor de betrokkene te beperken. Op die manier is het de betrokkene direct duidelijk of hij stappen dient te ondernemen.

Voorbeeld: In een niet-beveiligde directory op een server van de Nederlandse Energie Maatschappij (NEM) was een Excel bestand met de gebruikersnaam, e-mailadres en wachtwoord van 63.000 klanten toegankelijk. Met deze gegevens was het mogelijk om in te loggen op de persoonlijke pagina van de klanten. Via deze pagina wordt inzage gegeven in de naam- en adresgegevens, gegevens over het energieverbruik en de facturen van de klant. Enkele gegevens konden ook aangepast worden. In de melding aan de klant moet de verantwoordelijke aangegeven of het wachtwoord al is aangepast. [18] Heeft de verantwoordelijke dat nog niet gedaan dan moet de klant dat zo snel als mogelijk alsnog doen.

Melding moet betrokkene direct bereiken

19. Om te voorkomen dat een betrokkene op ongewenste wijze geconfronteerd wordt met de onbevoegde toegang tot zijn persoonsgegevens, is het noodzakelijk dat de betrokkene direct geïnformeerd wordt. Het heeft weinig zin om betrokkenen te informeren als zij eerder op een andere, onverwachte, manier al hebben ervaren dat hun persoonsgegevens zijn gelekt.

Voorbeeld: Op de website van de Amsterdamse taxicentrale kunnen klanten vertrouwelijk een klacht indienen. De bezoekers vullen daarbij persoonlijke gegevens in, zoals naam, e-mailadres en een telefoonnummer. Door een fout in de beveiliging van de website waren deze klachten, inclusief persoonsgegevens, publiek toegankelijk. [19] Als niet direct wordt gemeld kunnen klagers akelig verrast worden als chauffeurs hen met de klacht confronteren. Betrokkenen moeten dan ook direct geïnformeerd worden, zeker omdat de klachten over bedreigingen zeer ernstig zijn. [20]

20. Voor een effectieve melding is het noodzakelijk dat de verantwoordelijke de betrokkenen individueel benadert (zoals bijvoorbeeld met een bericht via e-mail of, in het geval van een kleine groep betrokkenen, per telefoon). Hierop mogen geen uitzonderingen zijn, ook niet als de melding een administratieve last met zich brengt. Als hierin technisch voorzien kan worden, dient de verantwoordelijke de aflevering van de melding te verifiëren. Als de aflevering niet gelukt is, moet opnieuw een poging ondernomen worden om de betrokkene individueel te benaderen. In aanvulling op deze persoonlijke melding dient er op de website van de door de gebruiker afgenomen dienst een duidelijk zichtbare melding opgenomen worden.

17 http://tweakers.net/nieuws/80123/hacker-steelt-wachtwoorden-338000-accounts-carrieresite.html
18 https://www.bof.nl/2010/12/20/datalek-nem-hoe-komen-al-je-gegevens-precies-op-straat-te-liggen/
19 https://www.bof.nl/2011/01/06/datalek-klachten-taxicentrale-openbaar/
20 http://www.dumpert.nl/mediabase/1281181/7b91aaf1/foutje._tca_maakt_taxiklachten_openbaar.html

Voorbeeld: Knus.nl is een website waarop 280.000 singles op zoek gaan naar een partner. Na een overhaaste aanpassing door de beheerders kregen ook leden onbedoeld toegang tot de interface voor beheerders. Zij konden op die manier door de profielen van alle leden bladeren. [21] Het is aannemelijk dat leden de website niet meer bezoeken als zij een partner gevonden hebben. Een melding van het lek op de website is dan ook niet afdoende om betrokkene te informeren dat hun hoogst persoonlijke profiel volledig toegankelijk is geweest voor derden. De betrokkene moet persoonlijk benaderd worden.

21. Enkel en alleen dan wanneer de organisatie niet in staat is om de betrokkenen te selecteren of indien contactgegevens ontbreken (bijvoorbeeld bij verlies van de databank met de persoons-gegevens) volstaat een niet-persoonlijke melding. In die situatie is de keuze van het medium afhankelijk van de betrokkenen die de verantwoordelijke probeert te bereiken. De inhoud van het en het medium voor de melding moet worden afgestemd op de groep van betrokkenen. Een inbreuk met gevolgen voor jongeren kan niet worden afgedaan met een advertentie in het Financieele Dagblad.

Uitzondering voor versleutelde informatie alleen indien niet omkeerbaar

22. Versleuteld zijn gegevens die, door gebruik te maken van een algoritmisch proces, omgezet zijn in een vorm waarin de gegevens onleesbaar of onbruikbaar zijn zonder gebruik van een vertrouwelijk proces of sleutel. De melding aan de betrokkene kan achterwege blijven indien deze versleuteling zodanig is dat deze nu en in de voorzienbare toekomst op geen enkele wijze ongedaan gemaakt kan worden zonder kennis van de geheime sleutel of proces en deze geheime sleutel of proces niet ook voor onbevoegden toegankelijk is of is geweest. Als het wachtwoord makkelijk te raden is, dan is hier geen sprake van. In de afgelopen twee jaar zijn tal van voorbeelden bekend waarbij de versleuteling onvoldoende bleek te zijn

Voorbeeld: Pepper is een betaalde website voor het vinden van een partner. Afgelopen zomer bleek de datingsite lek en lagen 53.000 gebruikersnamen, e-mailadressen en wachtwoorden op straat. Met deze gegevens is toegang te krijgen tot veel en gedetailleerde profielen. [22] De versleuteling van de wachtwoorden kon gemakkelijk ongedaan gemaakt worden. [23] Er zijn ook aanwijzingen dat dat inderdaad gebeurde.[24]

Voorbeeld: Ook de gegevens in databank van de Nederlandse Politiebond waren niet veilig. De gelekte gegevens omvatten onder meer de gebruikersnamen, versleutelde wachtwoorden en een aantal volledige namen. Omdat de versleuteling onvoldoende was waren de wachtwoorden betrekkelijk eenvoudig te herleiden. Daarmee waren ook de profielen van gebruikers op de website toegankelijk. [25]

23. Als onbevoegde toegang tot persoonsgegevens als uitgangspunt wordt gehanteerd, komen lid 6 en 7 overigens te vervallen.

21 https://www.bof.nl/2011/07/07/datalek-280-000-profielen-van-datingsite-toegankelijk/
22 https://www.bof.nl/2011/07/05/datalek-gedeelde-zoektocht-nieuwe-liefde/
23 http://webwereld.nl/nieuws/107200/hackers-misbruikten-configuratiefout-in-database-pepper-nl.html
24 http://webwereld.nl/nieuws/107188/wachtwoorden-pepper-nl-worden-actief-gekraakt.html
25 https://www.bof.nl/2011/07/11/datalek-ook-bij-politiebond-gegevens-niet-veilig/

Publiek register moet betrokkenen, verantwoordelijken en beleidsmakers informeren

24. Een publiek register van datalekken bevordert transparantie. Dat stelt anderen dan alleen de toezichthouder in staat onderzoek te doen naar de aard en de omvang van het probleem van datalekken. Dat leidt tot bewustzijn bij zowel betrokkenen als verantwoordelijken over de risico's die grootschalige opslag van persoonsgegevens met zich brengt. Media kunnen onderzoek doen naar bedrijfstakken met een onevenredig groot aantal of omvangrijke lekken. Betrokkenen kunnen een geïnformeerde keuze voor bepaalde bedrijven maken. Beleidsmakers in zowel de private als publieke sector kunnen leren van de ernst en de oorzaken van datalekken. Een publiek register stelt hen in staat beleid op feiten te baseren.

25. Een register bij het College is alleen zinvol als dat door iedereen geraadpleegd kan worden. Hieraan wordt niet voldaan als het College jaarlijks slechts enkele statistieken publiceert. Een register kan opgezet worden op dezelfde wijze als het meldingenregister, zoals bedoeld in artikel 30. Voor een optimale toegankelijkheid moet het register via een gebruiksvriendelijke website geraadpleegd kunnen worden. Goed onderzoek door derden kan worden gestimuleerd door het register toegankelijk te maken via een online interface (een API[26]). In de AMvB, zoals bedoeld in lid 11 van het voorgestelde artikel, kunnen regels gesteld worden met betrekking tot de publieke en vertrouwelijke onderdelen van de melding. Transparantie moet hierbij het uitgangspunt zijn.

26. Om zo'n publiek register te faciliteren moet het College worden geïnformeerd over i) het aantal betrokkenen van wie persoonsgegevens zijn gelekt, ii) de soort gelekte informatie en iii) de manier waarop de betrokkenen zijn geïnformeerd. Deze gegevens hoeven nu echter niet aan het College verstrekt te worden. Deze volledige informatie is noodzakelijk om de ernst van de inbreuk te kunnen beoordelen en om te kunnen controleren of aan de voorwaarden van lid 5, dat een behoorlijke en zorgvuldige informatievoorziening aan de betrokkenen moet waarborgen, is voldaan.

27. De relevante artikelen bevatten overigens ook enkele inconsistenties van meer cosmetische aard. Zo wordt in lid 3 gesproken over de maatregelen om “de gevolgen te beperken” terwijl in artikel 4 wordt gesproken over maatregelen om “de gevolgen te verhelpen”.

Voorstel aanpassingen artikel met onbevoegde toegang als grondbeginsel

28. Bits of Freedom is van mening dat onbevoegde toegang tot persoonsgegevens het criterium dient te zijn voor een melding aan de betrokkene en het College. Daarvoor is een andere formulering van het artikel noodzakelijk.

    Aan artikel 1 zou een lid toegevoegd moeten worden:

26 http://nl.wikipedia.org/wiki/Application_programming_interface

onbevoegde toegang: elke onbevoegde kennisneming van persoons gegevens

Artikel 34a komt te luiden:

1. De verantwoordelijke stelt de betrokkene en het College onverwijld in kennis als hij weet of vermoedt dat onbevoegde toegang is verkregen tot de door hem verwerkte persoonsgegevens.
2. De kennisgeving aan de betrokkene en het College omvat in ieder geval:
   a) de wijze waarop onbevoegde toegang is of vermoedelijk is verkregen,
   b) de aard van de persoonsgegevens waartoe onbevoegde toegang is of vermoedelijk is verkregen,
   c) de geconstateerde en vermoedelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene,
   d) de door de verantwoordelijke genomen of nog te nemen stappen om deze gevolgen te beperken,
   e) de aan de betrokkene aanbevolen maatregelen om deze gevolgen te beperken en
   f) de contactgegevens waaraan een verzoek om meer informatie kan worden gericht.
3. De kennisgeving aan het College omvat tevens een opgave van het aantal betrokkenen tot wiens persoonsgegevens onbevoegde toegang is of vermoedelijke is verkregen en een beschrijving van de wijze waarop de betrokkenen in kennis zijn gesteld.
4. De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de persoonsgegevens waartoe onbevoegde toegang is of vermoedelijk is verkregen, de geconstateerde en vermoedelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.
5. Het College houdt een register bij van de kennisgevingen als bedoeld in het eerste lid. Het register kan door een ieder kosteloos worden geraadpleegd.
6. Dit artikel is niet van toepassing voor zover
   a) de verantwoordelijke in zijn hoedanigheid als aanbieder van een elektronische communicatiedienst al een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, of
   b) op de verantwoordelijke een verplichting rust tot het verstrekken van informatie op grond van de artikelen 3:10, derde lid, of 4:11, vierde lid, van de Wet op het financieel toezicht.
7. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving en het register.

Voorstel aanpassingen artikel met zoveel als mogelijk aansluiting op huidige tekst

29. Mocht een herschrijving van het artikel niet mogelijk zijn, dan stelt Bits of Freedom de volgende wijzigingen voor. We hebben daarbij geprobeerd zoveel als mogelijk aan te sluiten bij de tekst van het ministerie.

Aan artikel 1 wordt een lid toegevoegd:

onbevoegde toegang: elke onbevoegde kennisneming van persoons gegevens

Artikel 34a komt te luiden:

1. De verantwoordelijke stelt het College onverwijld in kennis als hij weet of vermoedt dat onbevoegde toegang is verkregen tot de door hem verwerkte persoonsgegevens, danwel door een inbreuk op de maatregelen als bedoeld in artikel 13, danwel anderszins ~~van een inbreuk op de maatregelen, bedoeld in artikel 13, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden~~.
2. De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid.
3. De kennisgeving aan het College en de betrokkene omvat in ieder geval de aard van de inbreuk, de aard van de persoonsgegevens waartoe onbevoegde toegang is of vermoedelijk is verkregen, de geconstateerde en vermoedelijke gevolgen voor de betrokkene, de maatregelen die door de verantwoordelijke zijn genomen om de gevolgen te beperken, de contactgegevens waaraan een verzoek om meer informatie kan worden gericht ~~de instanties waar meer informatie over de inbreuk kan worden verkregen~~ en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
4. De kennisgeving aan het College omvat tevens het vermoedelijke aantal betrokkenen tot wiens gegevens onbevoegde toegang is of vermoedelijk is verkregen en de tekst en de vorm van de kennisgeving aan de betrokkene. ~~een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen~~.
5. De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.
6. ~~De kennisgeving aan de betrokkene is niet vereist indien de verantwoordelijke naar het oordeel van het College gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft versleuteld zijn of anderszins onbegrijpelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens.~~
7. ~~Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk nadelige gevolgen zal hebben voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.~~
8. Het College houdt een register bij van de kennisgevingen als bedoeld in het eerste lid. Het register kan door een ieder kosteloos worden geraadpleegd.
9. De verantwoordelijke houdt een overzicht bij van alle inbreuken. Dit overzicht bevat in elk geval de feiten en de gegevens, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.
10. Dit artikel is niet van toepassing voor zover de verantwoordelijke in zijn hoedanigheid als aanbieder van een elektronische communicatiedienst al een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.
11. Dit artikel is niet van toepassing indien op de verantwoordelijke een verplichting rust tot het verstrekken van informatie op grond van de artikelen 3:10, derde lid, of 4:11, vierde lid, van de Wet op het financieel toezicht.
12. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving en het register als bedoeld in lid 8.

Europese regelgeving onzeker en langdurig proces; nationale wetgeving doorzetten

30. Bits of Freedom verzoekt u het huidige voorstel door te zetten, ook nu in Europa onderhandelt wordt over de nieuwe verordening voor gegevensbescherming. Deze onderhandelingen zullen zonder twijfel een proces van lange duur zijn en het is onzeker wat het uiteindelijke resultaat zal zijn. Daarom moet Nederland niet wachten met de introductie van een meldplicht. Het Zwartboek Datalekken[27] en de voorbeelden hierboven tonen de urgentie van zo'n meldplicht aan. Bovendien heeft de regering in haar regeerakkoord toegezegd een meldplicht te introduceren.

31. Bits of Freedom ziet daarnaast graag dat u zich ook in Europa sterk maakt voor een effectieve meldplicht. De in deze brief genoemde elementen zorgen ervoor dat de betrokkene, tot wiens gegevens onbevoegde toegang is verkregen, zoveel als mogelijk de gevolgen van een datalek kunnen beperken. Op Europa niveau gelden dezelfde overwegingen.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Hoogachtend,

Rejo Zenger

27 https://www.bof.nl/category/zwartboek-datalekken/