



BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Position Paper
Meldplicht datalekken

25 januari 2010



BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Position Paper

Meldplicht datalekken

25 januari 2010

Over dit stuk

Bits of Freedom verdedigt communicatievrijheid en privacy in de informatiemaatschappij. Dit paper is geschreven door Bits of Freedom met medewerking van Koen Versmissen en anderen. Alleen Bits of Freedom is verantwoordelijk voor de inhoud en de eindredactie van dit paper.

Contact

Ot van Daalen
+31(0)654386680
ot.vandaalen@bof.nl

1. **SAMENVATTING**

1. Onze persoonsgegevens komen in steeds meer databanken voor. Die databanken zijn, mede doordat ze steeds vaker met internet verbonden zijn en doordat op een drager steeds meer gegevens kunnen worden opgeslagen, steeds moeilijker goed te beveiligen.
2. De kans op datalekken (het in verkeerde handen vallen van persoonsgegevens als gevolg van verlies of diefstal) neemt daardoor toe. Datalekken kunnen tegelijkertijd vergaande consequenties hebben voor betrokkenen: identiteitsfraude, ongewenste profilering, de-anonimisering en direct-marketing. Bovendien is verlies van vertrouwen in ICT een serieus risico van datalekken.
3. Om betrokkenen in staat te stellen hun schade te beperken zou de Nederlandse overheid volgens Bits of Freedom een verplichting om datalekken te melden moeten introduceren: een "meldplicht datalekken". Die meldplicht zou moeten gelden voor alle verwerkingen waarop betrokkenen een inzage- en correctierecht hebben, dus zou zowel voor bedrijfsleven, NGO's als de overheid moeten gelden. Datalekken zouden gemeld moeten worden aan (potentiële) slachtoffers en het College Bescherming Persoonsgegevens ("CBP"). Zowel vastgestelde als vermoede datalekken zouden onder de meldplicht vallen. De beperkte meldplicht zoals voorgeschreven in de ePrivacy-richtlijn is onvoldoende: het kabinet zou de herziening van de Wet bescherming Persoonsgegevens ("Wbp") moeten aangrijpen om een brede meldplicht op te nemen.
4. Dat wordt hieronder toegelicht.

2. **MEER PERSOONSgegevens WORDEN OPGESLAGEN IN DATABANKEN**

5. Meer en meer van onze persoonsgegevens vinden massaal hun weg naar grote databanken. Niet alleen omdat het steeds gemakkelijker en goedkoper wordt om persoonsgegevens elektronisch op te slaan, maar vooral ook doordat een steeds groter deel van ons leven zich online afspeelt. Met iedere stap die we online zetten laten we een digitaal spoor achter. Die gegevens kunnen eenvoudig worden opgeslagen en in theorie voor altijd met ons geassocieerd worden. In een onderzoek in opdracht van het CBP wordt geschat dat gegevens over de gemiddelde Nederlander in tussen de 250 en duizenden databanken zijn geregistreerd.¹
6. In het kader van verschillende projecten van de overheid worden uitgebreide gegevens over burgers opgeslagen. Telecomgegevens worden opgeslagen en toegankelijk gemaakt in het kader van de Wet bewaarplicht telecommunicatiegegevens. Reisdocumenten worden van biometrie voorzien, en deze biometrische kenmerken worden opgeslagen in databanken. Grote hoeveelheden privacygevoelige gegevens komen straks terecht in ons digitaal klantdossier in de sociale zekerheid, in ons elektronisch patiëntendossier en in het elektronisch kinddossier van onze kinderen. Dankzij de OV-chipkaart en straks de kilometerheffing (afhankelijk van de implementatie) zal ons reisgedrag tot in detail worden

¹ Zie voor meer informatie over deze thematiek bijvoorbeeld Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004) en Bart Schermer & Ton Wagemans, *Onze digitale schaduw: Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat* (Considerati, 2009).

geregistreerd en bewaard. Die bestanden worden vervolgens in toenemende mate aan elkaar gekoppeld.

7. Daarnaast legt de private sector grote databanken met informatie over hun klanten aan. Dat kunnen gegevens zijn die van de klant zelf verkregen zijn, maar het kan ook gaan om gegevens die van derden zijn verkregen (al of niet in strijd met de wet). Banken en winkels beschikken over uitgebreide databanken met de transacties van al hun klanten. Dienstverleners houden precies bij hoe hun klanten gebruik maken van hun dienst. Ook niet-commerciële instellingen houden grote databanken bij, bijvoorbeeld met adressen van donateurs.

3. DE KANS OP DATALEKKEN NEEMT TEGELIJKERTIJD TOE

8. Naarmate er meer en meer persoonsgegevens worden opgeslagen in steeds meer databanken, neemt ook de kans dat deze gegevens in verkeerde handen komen toe: "hoe meer je opslaat, hoe meer je kan kwijtraken". Er zijn daarnaast twee factoren die deze ontwikkeling versterken. In de eerste plaats maken organisaties databanken vaak (voor intern gebruik) toegankelijk via het internet. Het goed beveiligen van een databank is op zich al ingewikkeld, en als deze databanken aan het internet worden verbonden wordt dit extra moeilijk doordat deze voor meer mensen zichtbaar en toegankelijk worden. De kans op een inbraak of toevallige ontsluiting van data via internet neemt daarmee toe. Ten tweede passen er steeds meer gegevens op eenvoudig te vervoeren gegevensdragers zoals CD/DVD-ROMs en USB sticks. Geregeld worden er grote hoeveelheden gegevens uit databanken slecht of in het geheel niet beveiligd op zo'n mobiele gegevensdrager gezet, en het risico van misbruik bij verlies of diefstal wordt daarmee erg groot.
9. Ter illustratie worden hieronder een aantal in het oog springende casussen uit 2009 in Nederland gememoreerd:
 - In december 2009 is een USB-stick met de gegevens van 3.000 klanten van de Rabobank kwijtgeraakt. De stick bevatte persoonsgegevens, beleggingsvormen en in veel gevallen de hoogte van het belegde vermogen.²
 - Het adresboek van persbureau GPD bleek in augustus 2009 voor iedereen via Google beschikbaar te zijn gemaakt. Hierdoor zijn de telefoonnummers van bekende Nederlanders die een geheim nummer hebben, waaronder Geert Wilders en Gerard Spong, beschikbaar gekomen.
 - Het Dagblad van het Noorden heeft in mei 2009 meer dan 32.000 emailadressen van haar klanten per ongeluk toegankelijk gemaakt via haar website.³ De adressen zijn geïndexeerd in zoekmachines.
 - Door een fout in de website van de Geschillencommissie waren alle lopende en afgesloten dossiers tot 2005 online in te zien door personen die een geschil hadden lopen.⁴ Dit zijn tienduizenden geschillen. De dossiers bevatten gevoelige persoonsgegevens, zoals jaarafrekeningen, bankafschriften en NAW-gegevens. Pas in april 2009 is dit lek ontdekt door een journalist en de website is vervolgens off-line

2 Zie <http://www.gelderlander.nl/voorpagina/5961111/Bankgegevens-op-sstraat.ece>.

3 Zie <http://weblog.fok.nl/viewSingleItem/25294/Bedankt-Dagblad-vh-Noorden!.htm>.

4 Zie <http://nos.nl/artikel/85135-lek-in-beveiliging-geschillencommissie.html>.

gegaan.

- Een site waar gratis condooms konden worden besteld, maakte de gegevens van al haar klanten – ongeveer 10.000 – per ongeluk on-line beschikbaar. De site was juist bedoeld voor personen die zich schaamden om via een winkel condooms te kopen. Dit lek kwam in februari 2009 aan het licht.⁵

10. Ook in andere landen is dit een groot probleem: in de Verenigde Staten zijn bijvoorbeeld 316 incidenten geregistreerd in de “data loss database”. In totaal ging het om de gegevens van meer dan honderd miljoen personen. Het werkelijke aantal ligt waarschijnlijk veel hoger, aangezien bij veel incidenten onbekend is hoeveel gegevens zijn uitgelekt of gevaar liepen. Er zijn honderden vergelijkbare verhalen in andere landen. In het Verenigd Koninkrijk zijn in 2007 CD-rooms met de bankgegevens van 25 miljoen Engelsen (iedereen die recht heeft op kinderbijslag) kwijtgeraakt.⁶

4. DATALEKKEN KUNNEN GROOT PROBLEEM ZIJN VOOR BETROKKENEN

11. Datalekken brengen diverse risico's met zich, doordat de weggelekte gegevens op verschillende manieren oneigenlijk gebruikt kunnen worden.
 - Het belangrijkste risico van grote hoeveelheden gegevens die weglekken is identiteitsfraude. Persoonsgegevens zijn goud waard voor criminelen, die hiermee andermans identiteit aan kunnen nemen en zo fraude kunnen plegen. Identiteitsfraude is vaak een wat “onzichtbaar” fenomeen, aangezien vooral aandacht bestaat voor de misdrijven die volgen op identiteitsfraude, zoals het leeghalen van bankrekeningen. In de Verenigde Staten wordt identiteitsfraude niettemin al jarenlang erkend als een serieus probleem. In 2006 zijn meer dan 8 miljoen Amerikanen het slachtoffer geworden van identiteitsfraude. Ook in Nederland mag dit probleem zich langzamerhand verheugen in verhoogde aandacht, mede als gevolg van de grote media-aandacht voor de zaak van Ron Kowsoleea, die vijftien jaar lang last heeft gehad van het feit dat hij slachtoffer is van identiteitsfraude. Bij het Meldpunt Identiteitsfraude zijn in nog geen jaar tijd honderden meldingen van identiteitsfraude ontvangen. Dit lijkt erop te wijzen dat identiteitsfraude ook in Nederland een probleem van serieuze omvang is of aan het worden is.
 - Een tweede risico van deze datalekken is dat gebruikers met verkregen gegevens van bepaalde diensten kunnen worden uitgesloten, of op een andere manier nadelig behandeld kunnen worden. Zo kan je een verzekering geweigerd worden als door een lek bekend wordt dat je tot een risicogroep behoort. Omdat dit soort uitsluiting niet altijd wenselijk is, heeft de wetgever grenzen gesteld aan de persoonsgegevens die met het oog op dit soort selectie verwerkt mogen worden. Als gevolg van datalekken kunnen deze gegevens echter in sommige gevallen toch hun weg vinden naar plekken waar ze niet thuishoren. Het is goed voorstelbaar dat er handelsinformatiebureau's zijn die hiermee hun geld verdienen.
 - Een derde risico van deze datalekken, is dat de bewust gekozen anonimiteit van gebruikers hierdoor kan worden opgeheven. Gebruikers die hun identiteit slechts wilden delen met specifieke dienstverleners, zien gevoelige gegevens op straat liggen. Ook

5 Zie <http://www.nu.nl/internet/1914254/fout-onthult-klantendatabase-condoomgebruikers.html>

6 Zie <http://news.bbc.co.uk/2/hi/7103566.stm>.

kunnen gegevens die worden gelekt, soms in combinatie met reeds beschikbare gegevens leiden tot opheffing van anonimiteit: zo kon aan de hand van geanonimiseerde gebruikersinformatie die door een videoverhuurbedrijf op internet beschikbaar was gesteld, een vrouw toch geïdentificeerd worden (en ook haar seksuele geaardheid kon worden achterhaald).⁷

- Een vierde risico van deze datalekken, is het verlies van vertrouwen in ICT, waaronder e-commerce en e-banking. Gebruikers zullen steeds terughoudender zijn met het vertrouwen van hun gegevens aan dienstverleners, als zij niet weten wat vervolgens met die gegevens gebeurt, en als zij niet op de hoogte worden gesteld als het misgaat. Hierdoor zullen diensten die slechts verstrekt kunnen worden met behulp van deze gegevens, minder goed functioneren.
- Tot slot is het risico dat deze gegevens gebruikt worden om mensen ongevraagd te benaderen. Dat is vaak in strijd met wet- en regelgeving, maar dat weerhoudt bedrijven er vaak niet van om mensen te benaderen. Spam is hiervan een goed voorbeeld.

5. BETROKKENEN MOETEN WORDEN GEINFORMEERD OVER DATALEKKEN

12. Organisaties hebben er bij datalekken lang niet altijd belang bij om de slachtoffers daarvan op de hoogte te stellen. Niet alleen is het kwaad waar het de organisatie in kwestie betreft immers al geschied, ook kan deze in een ongunstig daglicht komen te staan wanneer breed bekend wordt dat er een datalek heeft plaatsgevonden. In de praktijk zijn er ook voorbeelden bekend van datalekken die (aanvankelijk) voor de slachtoffers verborgen werden gehouden.
13. Het is tegelijkertijd belangrijk dat slachtoffers snel op de hoogte worden gebracht van het feit dat persoonsgegevens van hen gecompromitteerd, of mogelijk gecompromitteerd zijn. Het tijdig en volledig informeren van slachtoffers van datalekken kan identiteitsfraude weliswaar niet geheel voorkomen, maar kan de slachtoffers wel in staat stellen om schadebeperkende maatregelen te nemen, zoals het laten blokkeren van hun credit card. En waar het niet mogelijk is om dit soort maatregelen te nemen, zal het informeren van de slachtoffers in ieder geval leiden tot verhoogde waakzaamheid, zodat bij het eerste teken van identiteitsfraude alsnog kan worden ingegrepen. De andere genoemde risico's van datalekken zullen in het algemeen minder gemakkelijk te voorkomen zijn door een slachtoffer dat op de hoogte is gebracht. Niettemin geldt ook daar dat bekendheid met het datalek tot verhoogde alertheid zal leiden, en daardoor zal helpen bij het blootleggen van het oneigenlijke gebruik van informatie.
14. Ook is het van belang dat organisaties meer open moeten zijn over datalekken. Indien zij niet alleen de slachtoffers moeten informeren, maar ook het algemene publiek, dan heeft dat verschillende positieve effecten:
 - Door bekendheid met de soort en hoeveelheid datalekken die voorkomen zullen burgers zich beter bewust worden van de gevaren van de opslag van hun gegevens in grote databanken, zeker als die slecht beveiligd worden. Dit stelt ze in staat om zich kritischer op te stellen jegens de beheerders van die databanken.

⁷ Zie http://www.volkskrant.nl/binnenland/article1329274.ece/Lesbische_moeder_daagt_online_videotheek_voor_de_rechter.

- Organisaties zullen uit angst voor reputatieschade hogere prioriteit geven aan goede beveiliging van de persoonsgegevens die zij beheren, opdat zij datalekken zoveel mogelijk kunnen voorkomen.
 - Ministeries, toezichthouders, brancheorganisaties en anderen zullen zo kunnen beschikken over actuele en volledige beleidsinformatie over datalekken.
15. Het is dan ook niet verbazingwekkend dat in verschillende landen en in Nederland de roep om een meldplicht datalekken toeneemt. De meldplicht datalekken is al in meerdere landen geïntroduceerd, waaronder onlangs in Duitsland (zie onder meer het rapport “Melding Maken” van Research voor Beleid, gepubliceerd op 17 april 2009, voor een deeloverzicht hiervan). Op Europees niveau wordt deze meldplicht datalekken in het kader van de herziening van de ePrivacy-richtlijn (2002/58/EG) ingevoerd, maar die geldt slechts voor de telecommunicatiesector. Bovendien pleit de Artikel 29-werkgroep voor een vergelijkbare meldplicht (zie opinie 1/2009 van 10 februari 2009). Peter Hustinx van de Europese toezichthouder voor persoonsgegevens heeft in 2008 opgeroepen tot een bredere meldplicht voor datalekken.⁸ Officier van justitie Speijers, CBP-voorzitter Kohnstamm en D66-leider Pechtold hebben in 2008 ook opgeroepen tot een wettelijke meldplicht bij diefstal van persoonsgegevens van klanten.⁹ Ook de PvdA wil een meldplicht instellen voor grote bedrijven na inbraak in hun computersystemen.¹⁰
16. Hoewel reeds een beperkte meldplicht voor telecomaانبieders in de ePrivacy-richtlijn is opgenomen, is de door Bits of Freedom voorgestelde meldplicht breder: deze ziet op alle soorten databanken. Er is in de media te lezen dat op Europees niveau een bredere meldplicht in de maak is. Het duurt echter te lang om daarop te wachten: Nederland kan de implementatie van de herziening van de ePrivacy richtlijn aangrijpen om een brede meldplicht op te nemen. Dat zou passen in het beleid zoals aangekondigd in de brief van de Minister van Binnenlandse Zaken van 8 april 2009 aan de Tweede Kamer, waarin wordt aangekondigd dat het kabinet “na afronding van de besluitvorming op Europees niveau [zal] overgaan tot nationale implementatie en een meldplicht [zal] invoeren in geval van verlies van persoonsgegevens uit datasystemen”. Daarbij zal gebruik worden gemaakt van de kennis die is opgedaan uit het rapport “Melding maken?”. Daarom zou het kabinet reeds nu een meldplicht datalekken volgens de volgende richtlijnen moeten introduceren.

A.1 Wie moet melden?

Zoals we hebben gezien ontstaan er op steeds meer plaatsen grote databanken: zowel in de publieke als de private sector. Bits of Freedom vindt dan ook dat de meldplicht datalekken voor alle organisaties moet gelden. Of, in termen van de Wet bescherming persoonsgegevens: een meldplicht datalekken geldt voor alle verantwoordelijken.

A.2 Bij wie moet er gemeld worden?

(Mogelijke) datalekken moeten in beginsel worden gemeld bij zowel de (mogelijke) slachtoffers als bij een onafhankelijk overheidsorgaan. Gelet op de noodzakelijke breedte van de meldplicht en het feit dat het om, vaak gevoelige, persoonsgegevens gaat, vindt Bits of Freedom dat het bijhouden van meldingen het beste bij het College Bescherming

8 Zie <http://webwereld.nl/nieuws/50725/eu-waakhond-pleit-voor-meldplicht-informatielekken.html>.

9 Zie <http://webwereld.nl/nieuws/53492/roep-om-meldplicht-datalekken-zwelt-aan.html>.

10 Zie <http://webwereld.nl/nieuws/50548/pvda-wil-meldplicht-computercriminaliteit.html>.

Persoonsgegevens kan worden neergelegd.

A.3 Wat voor soort datalekken moeten gemeld worden?

Bits of Freedom vindt dat zowel vastgestelde datalekken als vermoede datalekken moeten worden gemeld. Met vermoede datalekken bedoelen we beveiligingsinbreuken waarvan niet duidelijk is of als gevolg daarvan ook persoonsgegevens in verkeerde handen terecht zijn gekomen. Verder doet het er in de ogen van Bits of Freedom niet toe hoeveel of wat voor gegevens er zijn ontvreemd: alle datalekken zouden meldingsplichtig moeten zijn.

A.4 Tekstvoorstel wijziging Wbp

Aan de Wet bescherming persoonsgegevens (Wbp) wordt een artikel 13a toegevoegd, dat als volgt luidt:

1. De verantwoordelijke die weet, of redelijkerwijs kan vermoeden, dat onbevoegd toegang is verkregen tot door hem verwerkte persoonsgegevens, stelt de betrokkenen daarvan onverwijld op de hoogte.
2. De verantwoordelijke als bedoeld in het eerste lid stelt eveneens het College onverwijld op de hoogte.
3. Het College houdt een openbaar register bij van de meldingen die het ontvangt uit hoofde van het tweede lid.
4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over de wijze waarop de meldingen dienen te geschieden.

Aan de lijst van artikelen in artikel 15 Wbp wordt het nieuwe artikel 13a toegevoegd. In de toelichting dient duidelijk gemaakt te worden dat de zinsnede “redelijkerwijs kan vermoeden” ook van toepassing is op beveiligingsinbreuken waarvan niet bekend is of die tot onbevoegde toegang tot gegevens hebben geleid. Met “onbevoegde toegang” wordt bedoeld op toegang die is verkregen in strijd met technische beveiligingsmaatregelen of juridische waarborgen. De verantwoordelijk moet de betrokkenene op de hoogte stellen van de specifieke persoonsgegevens waartoe mogelijk onbevoegd toegang is verkregen. Het is dus niet voldoende om alleen te melden *dat* onbevoegd toegang is gekregen.

Daarnaast zou de Nederlandse overheid bedrijven en organisaties moeten ondersteunen bij de stappen die ze moeten nemen als sprake is van een datalek. In de Verenigde Staten bestaat al veel ervaring met “data breaches”. De Federal Trade Commission biedt actieve ondersteuning aan bedrijven en organisaties die betrokken zijn bij een datalek, onder meer door voorlichting via haar website.¹¹ De gedachte hierachter is dat een meldplicht niet alleen een sanctie is voor slechte beveiliging, maar dat het ook bedoeld is om verdere schade te voorkomen. Bedrijven en organisaties die geholpen worden met het snel informeren van slachtoffers, zullen zo meer schade kunnen voorkomen.