Mr. J.A.N. Baas en mr. M.H.J. van Rest[*]

Informatie- en meldplichten bij datalekken en beveiligingsinbreuken

228

Trefwoorden:
datalek, beveiligingsinbreuk, meldplicht, informatieplicht

Dit artikel beschrijft de informatie- en meldplichten die gelden bij datalekken en beveiligingsinbreuken. Allereerst wordt kort ingegaan op expliciete wettelijke meldplichten die nu gelden en in de toekomst mogelijk worden ingevoerd. In paragraaf 2 wordt de melding aan toezichthoudende autoriteiten en betrokkene behandeld en in paragraaf 3 de verhouding tussen de verantwoordelijke, de bewerker en een mogelijke derde. In de rest van het artikel wordt onderzocht in hoeverre op dit moment, ondanks het ontbreken van een expliciete wettelijke verplichting daartoe, al een verplichting bestaat om een datalek of beveiligingsinbreuk aan de betrokkene te melden.

1 Datalekken en beveiligingsinbreuken

Datalekken en beveiligingsinbreuken komen steeds vaker in het nieuws. Zo werd afgelopen 6 juni bekend dat 6,5 miljoen wachtwoorden van LinkedIn op straat lagen. In februari werd ingebroken in de databank van carrièreadviesbureau Nobiles Media. De gehele databank met 338 000 accounts werd gekopieerd. De hacker zette vervolgens van 900 mensen gegevens zoals naam, adresgegevens, e-mail en wachtwoord op internet.[1]

Dergelijke incidenten zijn voor de betrokken organisaties een publicitaire ramp. De eerste reflex zal daarom misschien zijn om het probleem niet aan de grote klok te hangen. Daarmee neemt de getroffen organisatie een risico, zoals is gebleken in de casus 'DigiNotar'. Hoewel de beveiligingsinbreuk bij dit bedrijf niet rechtstreeks betrekking had op persoonsgegevens[2] illustreert deze casus wel goed het dilemma waar een organisatie voor komt te staan als een beveiligingsinbreuk of datalek wordt geconstateerd. Het verwijt dat DigiNotar trof was niet alleen dat vervalste beveiligingscertificaten in omloop waren geraakt, maar ook dat zij de gevolgen hiervan had verergerd en vertrouwen had geschaad door het probleem stil te houden. Een organisatie die wordt geconfronteerd met een beveiligingsinbreuk of datalek zal zorgvuldig moeten afwegen of het niet alleen al om verergering van het probleem te voorkomen de voorkeur verdient om open kaart te spelen.

De vraag die aan de juridische adviseur van de organisatie zal worden gesteld is of er ook een wettelijke verplichting bestaat om een datalek of beveiligingsinbreuk te melden, aan een toezichthoudende autoriteit, aan de betrokkene(n) of aan derden. Dit is de vraag die dit artikel probeert te beantwoorden.

Het wekt geen verbazing dat de incidenten die in de media zijn gekomen ook tot politieke onrust hebben geleid en tot initiatieven om tot wettelijke meldplichten te komen. Hieronder zal kort worden ingegaan op deze initiatieven. In hoofdzaak zal echter worden besproken welke meldplichten reeds volgen uit het thans geldende recht.

In dit artikel wordt onderscheid gemaakt tussen beveiligingsinbreuken (een inbreuk op beveiligingsmaatregelen zoals deze onder andere worden vereist in art. 13 Wbp) en datalekken (beveiligingsinbreuken en andere incidenten waarbij daadwerkelijk persoonsgegevens in handen van onbevoegden zijn gekomen).

2 Melding aan toezichthoudende autoriteiten

2.1 *Geldende regelgeving*

De Wbp kent op dit moment geen verplichting tot het melden van beveiligingsinbreuken of datalekken aan toezichthoudende autoriteiten.

Op 5 juni 2012 is het nieuwe art. 11.3a Telecommunicatiewet (hierna: 'Tw') in werking getreden.[3] Door dit artikel zijn aanbieders van openbare elektronische communicatienetwerken en -diensten verplicht om een inbreuk op de beveiligingsmaatregelen die zij hebben genomen

---

* **Jan Baas en Marjolein van Rest zijn advocaat bij BarentsKrans te Den Haag.**

1 Voor meer praktijkgevallen van datalekken, zie het *Zwartboek Datalekken* van Bits of Freedom: www.bof.nl/category/zwartboek-datalekken.

2 DigiNotar verstrekte certificaten waarmee de herkomst van een site gecontroleerd kon worden. Door hackers werden vervolgens valse certificaten afgegeven waardoor niet meer gegarandeerd kon worden dat een site afkomstig was van bijvoorbeeld de overheid. Indirect konden hierdoor persoonsgegevens in het geding zijn omdat mensen mogelijk hun persoonsgegevens invulden op een verkeerde site.

3 Het wetsvoorstel dient ter implementatie van art. 4 lid 3 Richtlijn 2002/58/EG (e-Privacyrichtlijn). Zie voor deze meldplicht in de Tw uitgebreid: F.J. Zuiderveen Borgesius, 'De meldplicht voor datalekken in de Telecomwet', *Computerrecht* 2011, p. 291.

te melden bij de OPTA[4] wanneer die inbreuk nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.

De aanbieder dient blijkens lid 2 ook degene wiens persoonsgegevens het betreft in te lichten wanneer de inbreuk in verband met de persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Op grond van art. 3:17 en 4:15 Wet op het financieel toezicht (hierna: 'Wft') zijn financiële ondernemingen verplicht hun bedrijfsvoering zodanig in te richten dat deze een beheerste en integere uitvoering van hun bedrijf waarborgt.[5] Incidenten die betrekking hebben op de integere bedrijfsuitoefening moeten op grond van art. 3:10 lid 3 en art. 4:11 lid 4 Wft aan DNB of de AFM gemeld worden.[6] Onder zulke incidenten vallen naar mag worden aangenomen mede datalekken en beveiligingsinbreuken.[7]

Het is daarnaast goed denkbaar dat een datalek of een beveiligingsinbreuk gepaard gaat met strafbare feiten. Zo is schending van de geheimhoudingsplicht van art. 12 lid 2 Wbp een strafbaar feit (art. 272 Sr). Dit geldt bijvoorbeeld ook voor het verbreken van beveiligingsmaatregelen zoals bedoeld in art. 13 Wbp (art. 138ab Sr 'computervredebreuk'). Er bestaat in deze gevallen echter geen algemene verplichting om strafrechtelijke aangifte te doen. Alleen art. 160 Sv bevat een aangifteplicht, maar deze heeft betrekking op misdrijven tegen de veiligheid van de staat, misdrijven tegen de koninklijke waardigheid, misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht voor zover daardoor levensgevaar is veroorzaakt, misdrijven tegen het leven gericht, afbreking van zwangerschap, ontvoering en verkrachting. Naar aanleiding van de beveiligingsinbreuk bij DigiNotar is wel betoogd dat er in dat geval een aangifteverplichting bestond omdat mensenlevens in gevaar zijn gebracht.[8] Ofschoon de suggestie in het aangehaalde artikel (door anonieme strafrechtdeskundigen) in de casus DigiNotar mogelijk wat ver gaat zijn er casussen denkbaar waarin een beveiligingsinbreuk of datalek kan leiden tot een strafrechtelijke aangifteverplichting.[9]

2.2 *Toekomstige regelgeving nationaal*

In de Wet bescherming persoonsgegevens wordt in de toekomst mogelijk een algemeen geldende meldplicht ingevoerd. Op 20 december 2011 heeft staatssecretaris Teeven een consultatievoorstel gepubliceerd (hierna: 'het Consultatievoorstel') waarin hiertoe onder andere een nieuw art. 34a Wbp is opgenomen.[10] Inmiddels heeft de Raad van State advies uitgebracht over een wetsvoorstel, maar dit advies en de tekst van het wetsvoorstel worden pas openbaar bij indiening bij de Tweede Kamer.[11] In het navolgende gaan wij uit van de tekst van het Consultatievoorstel.

Het voorgestelde art. 34a Wbp bevat een algemene meldplicht voor een verantwoordelijke: deze moet het CBP onverwijld in kennis stellen van een inbreuk op de beveiligingsmaatregelen waarvan redelijkerwijs kan worden aangenomen dat deze 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.

Daarnaast moet de verantwoordelijke ingevolge lid 2 ook de betrokkene onverwijld van een dergelijke inbreuk op de hoogte stellen. De kennisgeving aan de betrokkene dient op zodanige wijze gedaan te worden 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'. Blijkens de toelichting bij het Consultatievoorstel kan op grond hiervan bij een groot aantal getroffenen bijvoorbeeld worden afgezien van persoonlijke en gerichte benadering en kan worden volstaan met vermelding op een website en het plaatsen van een advertentie in de dagbladen.

Wanneer naar het oordeel van het CBP redelijkerwijs is uitgesloten dat het datalek kan leiden tot kennisname van persoonsgegevens door onbevoegden (bijvoorbeeld door encryptie), kan melding aan de betrokkene achterwege blijven.[12]

---

4 In het Consultatievoorstel (zie par. 2.2) wordt dit gewijzigd in CBP.
5 In art. 20 lid 2 Besluit prudentiële regels Wft en art. 30 lid 4 Besluit gedragstoezicht financiële ondernemingen Wft is vervolgens een beveiligingsverplichting opgenomen die gelijkenissen vertoont met art. 13 Wbp.
6 De financiële onderneming dient deze incidenten ook intern vast te leggen op grond van art. 12 Besluit prudentiële regels Wft en art. 19 Besluit gedragstoezicht financiële ondernemingen Wft.
7 Zie J.M.A. Berkvens, 'Datalekken in de financiële sector', *Tijdschrift voor financieel recht* 2011, p. 382.
8 www.nu.nl/internet/2605567/diginotar-deed-geen-aangifte-hack.html.
9 Zie over dit onderwerp uitgebreider R. van Staden ten Brink, 'Cybercrime, wie stellen we op de hoogte?', *Tijdschrift voor Sanctierecht en compliance* 2011, p. 5. Van Staden ten Brink gaat ook in op de voor- en nadelen van vrijwillige samenwerking met politie en justitie.
10 Te vinden via www.internetconsultatie.nl/camerabeelden. De consultatie is op 29 februari 2012 gesloten. In het wetsvoorstel is ook een regeling opgenomen voor een verruiming van het gebruik van camerabeelden gemaakt met particuliere beveiligingscamera's van burgers en bedrijven ten behoeve van de opsporing van strafbare feiten. Zie omtrent de meldplicht nader F. van der Jagt, 'Iets te melden? De diverse datalekmeldplichten in kaart gebracht', *NJB* 2012, p. 1713. Van der Jagt geeft tevens een praktisch schematisch overzicht van de huidige en (mogelijke) toekomstige meldplichten en gaat uitgebreider dan wij in dit artikel doen in op de toekomstige ontwikkelingen.
11 Persbericht Rijksoverheid d.d. 13 juli 2012, zie www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2012/07/13/beelden-van-bewakingscamera-s-meer-inzetten-bij-opsporing.html.
12 Zie art. 34a lid 6 Wbp.

In april bleek dat medische gegevens van honderdduizenden Nederlanders maandenlang konden worden ingezien via een lek in de website Humannet van IT-bedrijf VCD. Journalisten van het VARA-programma Zembla ontdekten dat de meer dan 300 000 personeels- en medische dossiers die beheerd worden via de verzuimsoftware van Humannet al maanden slecht beveiligd waren. Via het lek was het eenvoudig om inlognamen en wachtwoorden te achterhalen, waarna databases met gegevens over het verzuim van 300 000 werknemers toegankelijk waren. Het ging om contactgegevens en informatie over herstel en re-integratie van medewerkers van honderden bedrijven, zoals FC Twente, de gemeente Deventer, Praxis, Bijenkorf, V&D, Hornbach, Beter Bed en Action. Daarnaast waren medische dossiers van bedrijfsartsen en burgerservicenummers op te vragen. De journalisten konden zien hoe het met de gezondheid van de spelers van FC Twente gaat, maar ook wat een bekende oud-international verdient als hulptrainer van Go Ahead Eagles.

2.3 *Toekomstige regelgeving Europees*

Ook op Europees niveau wordt nagedacht over de invoering van een meldplicht voor datalekken en beveiligingsinbreuken. In het Commissievoorstel voor een Verordening gegevensbescherming (hierna: 'de Conceptverordening') is een dergelijke meldplicht opgenomen in art. 31 en 32.[13] Op grond van art. 31 is de verantwoordelijke verplicht een inbreuk in verband met persoonsgegevens te melden aan de toezichthoudende autoriteit.

Wanneer de inbreuk waarschijnlijk negatieve gevolgen voor de bescherming van de persoonsgegevens of de privacy van de betrokkene heeft, moet de inbreuk na de melding aan de toezichthoudende autoriteit ook gemeld worden aan de betrokkene zelf.[14]

3 Meldplicht bewerker jegens verantwoordelijke/ verantwoordelijke jegens derden

3.1 *Bewerker jegens verantwoordelijke*

Op grond van art. 14 Wbp dient de verantwoordelijke ervoor zorg te dragen dat een bewerker de beveiligingsverplichting van art. 13 Wbp nakomt. De uitvoering van verwerkingen door een bewerker moet worden vastgelegd in een overeenkomst tussen de bewerker en de verantwoordelijke. In de Wbp is geen expliciete verplichting opgenomen voor de bewerker om een beveiligingsinbreuk of datalek aan de verantwoordelijke te melden. Een dergelijke verplichting volgt mogelijk wel uit art. 6:248, 7:401 en 7:403 BW. Om onduidelijkheid op dit punt te voorkomen is het (vanuit het perspectief van de verantwoordelijke) aan te bevelen om in de overeenkomst een expliciete verplichting op te nemen voor de bewerker om beveiligingsinbreuken of datalekken aan de verantwoordelijke te melden, al dan niet onder verbeurte van een boete in geval van niet-nakoming. Dit om als verantwoordelijke deugdelijk te kunnen controleren of de bewerker zijn beveiligingsverplichtingen nakomt en om in geval van incidenten adequaat te kunnen reageren.

In het Consultatievoorstel wordt een nieuw onderdeel c aan art. 14 lid 3 Wbp toegevoegd. Ingevolge dit artikel dient de verantwoordelijke ervoor te zorgen dat de bewerker de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de meldplicht. De verantwoordelijke heeft er na invoering van het Consultatievoorstel dus temeer belang bij om adequaat door de bewerker te worden geïnformeerd in geval van een beveiligingsinbreuk of datalek. De tekst van het nieuwe art. 14 lid 3 Wbp lijkt er overigens van uit te gaan dat het in alle gevallen de bewerker is die de melding doet.[15] Wij kunnen ons voorstellen dat de verantwoordelijke dit onder omstandigheden zelf wil doen. De wettelijke regeling dient daar ruimte voor te laten.

De Conceptverordening legt de verantwoordelijkheid eveneens bij de verantwoordelijke, maar verplicht de bewerker tevens om de verantwoordelijke te waarschuwen en te informeren in geval van een datalek (art. 31 lid 2) en om de verantwoordelijke te ondersteunen in de nakoming van zijn verplichtingen op dit punt (art. 26 lid 2 onder f). Dit zou wat ons betreft ook uitgangspunt van een Nederlandse regeling dienen te zijn.

3.2 *Verantwoordelijke jegens derden*

Er bestaan vele contractuele verhoudingen waarbij de verwerking van persoonsgegevens een rol speelt maar waarbij partijen niet tegenover elkaar staan als verantwoordelijke en bewerker. Denk aan de relatie tussen een pensioenadviesbureau en een opdrachtgever of aan twee bedrijven die in samenwerking producten of diensten aanbieden, bijvoorbeeld in geval van een aanbieding met uitgestelde betaling waarbij een kredietinstelling financiert. Ook in dergelijke situaties kunnen op grond van die contractuele verhouding meldplichten bij datalekken of beveiligingsinbreuken bestaan, bijvoorbeeld ingevolge

13 Zie Com(2012)11 def. Zie over deze Conceptverordening in het algemeen: J.M. Titulaer-Meddens, 'De Algemene verordening gegevensbescherming en het bedrijfsleven', *P&I* 2012, p. 100-109, zie m.b.t. de meldplicht par. 2.9 van haar artikel; zie voorts Van der Jagt 2012, *supra* noot 10.

14 Art. 32 Conceptverordening.

15 Zie ook het voorgestelde art. 14 lid 5 Wbp op grond waarvan de verplichting tot melding ook in de bewerkersovereenkomst vastgelegd dient te worden.

art. 6:248, 7:401 of 7:403 BW. Om onduidelijkheden te voorkomen is het ook in deze verhoudingen verstandig om dit punt expliciet te regelen in de overeenkomst.

4 Meldplicht jegens betrokkene

4.1 *Inleiding*

De huidige wet- en regelgeving bevat geen expliciete verplichting om een beveiligingsinbreuk of datalek te melden aan betrokkenen, behoudens het in paragraaf 2.1 besproken art. 11.3a lid 2 Telecommunicatiewet. Deze verplichting geldt slechts voor aanbieders van openbare elektronische communicatienetwerken en -diensten. Daarnaast worden bij invoering van het Consultatievoorstel of de Conceptverordening in de toekomst mogelijk algemeen geldende meldplichten jegens betrokkenen ingevoerd. In paragraaf 2.2 en 2.3 zijn deze reeds kort besproken. Op dit moment is dat nog toekomstmuziek.

De vraag is of een dergelijke verplichting desondanks kan worden geconstrueerd aan de hand van art. 6, 33 en 34 Wbp, art. 6:162 BW (onrechtmatige daad), art. 6:248 lid 1 BW (verplichtingen voortvloeiende uit overeenkomst), art. 7:401 BW (zorgplicht goed opdrachtnemer), art. 7:403 BW (informatieplicht opdrachtnemer) of art. 7:611 BW (goed werkgeverschap). Hierover hebben wij geen rechtspraak of literatuur aangetroffen, behoudens het hierboven reeds aangehaalde artikel van Berkvens,[16] die stelt:

'Op dit moment geldt voor de financiële sector evenals voor andere sectoren al de generieke meldplicht van art. 6 Wbp en art. 33 Wbp richting klant bij relevante incidenten'.

Berkvens licht deze stelling in zijn artikel niet nader toe. In de toelichting bij het Consultatievoorstel wordt daarnaast, eveneens zonder nadere onderbouwing of verwijzing naar wetsartikelen, gesteld dat 'financiële ondernemingen hun cliënten zo spoedig mogelijk informeren over het incident, wanneer dat gevolgen heeft of heeft gehad voor de desbetreffende cliënt'.[17] In deze memorie wordt derhalve blijkbaar ook uitgegaan van een in bepaalde gevallen bestaande meldplicht jegens de betrokkenen.

Van der Jagt noemt in een recent artikel art. 6, 33 en 34 Wbp en art. 6:162, 6:248 en 7:401 BW als mogelijke grondslagen voor een meldplicht, eveneens zonder deze grondslagen nader uit te diepen.[18]

In het hiernavolgende wordt nader onderzocht in hoeverre er in geval van een datalek een verplichting bestaat dit aan de betrokkene te melden. Hiertoe worden eerst de mogelijke grondslagen algemeen besproken, waarna vervolgens nader ingegaan zal worden op de vraag in welke concrete gevallen een verplichting bestaat.

Een beveiligingsinbreuk als zodanig (waarbij vaststaat dat geen persoonsgegevens zijn gelekt) zal over het algemeen geen aanleiding hoeven geven voor een mededeling aan de betrokkene nu diens belangen hierdoor in beginsel niet worden geraakt. Dit kan anders zijn indien wel het risico bestaat dat persoonsgegevens zijn gelekt. Dit is eveneens uitgangspunt in de reeds ingevoerde en toekomstige wettelijke regelingen.

4.2 *Art. 33 en 34 Wbp*

Op grond van art. 33 en 34 Wbp is de verantwoordelijke gehouden om de betrokkene te informeren over zijn identiteit en de doeleinden van de verwerking. Daarnaast dient nadere informatie verstrekt te worden voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

De verantwoordelijke die de persoonsgegevens verkrijgt van de betrokkene is gehouden om deze te informeren vóór het moment van verkrijgen van de persoonsgegevens. De verantwoordelijke die de persoonsgegevens verkrijgt van een derde is gehouden om de betrokkene te informeren op het moment van vastlegging van de gegevens of, indien de gegevens zijn bestemd om te worden verstrekt aan een (andere) derde, uiterlijk op het moment van eerste verstrekking.

De vraag is of deze verplichting is uitgewerkt nadat de informatie eenmaal is verstrekt, of dat er een nieuwe verplichting tot informeren kan ontstaan indien omstandigheden daartoe aanleiding geven. De wettekst, mede in het licht van de tekst van de relevante bepalingen uit de Richtlijn Bescherming Persoonsgegevens,[19] pleit voor de eerste opvatting. Ook de wetsgeschiedenis is hierover zeer expliciet:

'Als aan de informatieplicht overeenkomstig de artikelen 33 of 34 is voldaan, zijn deze artikelen uitgewerkt en zal er ook geen sprake meer kunnen zijn van een onrechtmatige verkrijging wegens niet nakoming van deze plicht'.[20]

Verderop in de memorie van toelichting is weliswaar te lezen:

16 Berkvens 2011, *supra* noot 7, p. 382.
17 Zie p. 11 van de toelichting bij het Consultatievoorstel.
18 Van der Jagt 2012, *supra* noot 10, p. 382.
19 Richtlijn 95/46/EG. Waarbij overigens wel wordt opgemerkt dat art. 10 van de richtlijn (informatieplicht in het geval dat de gegevens van de betrokkene zelf worden verkregen) geen tijdstip noemt. Vgl. tevens Chr. Kuner, *European Data Protection Law*, New York: OUP 2007, p. 293, die het 'doubtful' noemt of art. 10 van de richtlijn verplichtingen met zich meebrengt om een datalek te melden.
20 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 154-155.

'(…) Wel is het denkbaar dat specifieke omstandigheden met zich meebrengen dat informatie moet worden verstrekt om een "behoorlijke en zorgvuldige verwerking" te waarborgen. Daarbij valt te denken aan latere ontwikkelingen van zodanige aard, dat zij aan de betrokkene bij de verkrijging hadden moeten worden medegedeeld, indien zij op dat tijdstip bekend waren geweest'.

Met de woorden 'behoorlijke en zorgvuldige verwerking' wordt echter verwezen naar art. 6 Wbp en niet naar art. 33 en 34 Wbp. Op zich komen deze woorden ook voor in lid 3 van art. 33 Wbp, dat vereist dat nadere informatie wordt verstrekt voor zover dat nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen. Het tijdstip van verstrekking van de in lid 3 bedoelde nadere informatie is echter gekoppeld aan de in art. 33 lid 1 en art. 34 lid 1 bedoelde momenten. Dit wordt bevestigd in een uitspraak van het CBP van 4 maart 2003, hierna aan te duiden als 'de UWV-uitspraak'.[21] Het UWV had zonder medeweten en zonder toestemming van verzoekster haar dossier, met daarin zowel medische als sociale gegevens, verstrekt aan een bedrijfsarts werkzaam bij een private organisatie. Het CBP is van oordeel dat verzoekster door het UWV geïnformeerd had moeten worden over het inschakelen van bedrijfsartsen van dit bedrijf. Volgens het CBP volgt deze informatieplicht gezien de reikwijdte van art. 33 Wbp uit art. 6 Wbp. Het CBP beroept zich in dit verband mede op de hierboven aangehaalde passage uit de wetsgeschiedenis.

Onze conclusie is op basis van het voorgaande dat een meldplicht aan de betrokkene niet kan worden gebaseerd op art. 33 en 34 Wbp. Wij hebben nog nagedacht over de vraag of dit anders is indien in eerste instantie van informeren van de betrokkene is afgezien omdat een van de uitzonderingen van art. 33 en 34 Wbp zich voordeed (de betrokkene is al op de hoogte, onevenredige inspanning). Het ligt in onze ogen voor de hand om aan te nemen dat ook in het geval dat op het moment dat de informatie ingevolge art. 33 en 34 Wbp verstrekt zou dienen te worden, maar hiervan ingevolge een van de uitzonderingen van afgezien kan worden, de informatieplicht is uitgewerkt en de verplichting dit te melden aan de betrokkenen niet in het kader van art. 33 en 34 Wbp beoordeeld dient te worden.

4.3 *Art. 6 Wbp*

Op grond van art. 6 Wbp dienen persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze te worden verwerkt. Het artikel implementeert art. 6 lid 1 onder a van de Richtlijn Bescherming Persoonsgegevens, dat vereist dat persoonsgegevens 'eerlijk en rechtmatig' moeten worden verwerkt.

De Nederlandse wetgever heeft ervoor gekozen om het begrip 'eerlijk' (of 'fair') niet in de Nederlandse wet over te nemen omdat dit vereiste reeds is geïncorporeerd in het onrechtmatigheidscriterium van art. 6:162 BW. Met het woord 'zorgvuldig' beoogde de wetgever aan te sluiten bij de zorgvuldigheidsnorm van art. 6:162 BW (handelen in strijd met hetgeen volgens ongeschreven regels in het maatschappelijk verkeer betaamt) en het zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur. Het begrip 'behoorlijk' verwijst naar het behoorlijkheidsbeginsel als algemeen beginsel van behoorlijk bestuur.[22] De Nederlandse wetgever beoogde derhalve bij de invoering van art. 6 Wbp geen nieuwe zelfstandige normstelling. Aangenomen mag worden dat een overtreding van de zorgvuldigheidsnorm uit art. 6 Wbp mede een handelen oplevert in strijd met hetgeen volgens ongeschreven regels in het maatschappelijk verkeer betaamt, en vice versa.

Art. 6 Wbp is ondanks het ontbreken van een dergelijke zelfstandige normstelling uiteraard niet betekenisloos, in het bijzonder omdat het in geval van een onrechtmatige gegevensverwerking de publiekrechtelijke bevoegdheden van het CBP activeert en een betrokkene naar aanleiding van overtreding gebruik kan maken van de rechten die de Wbp hem biedt, zoals de mogelijkheid van het instellen van de vorderingen van art. 49 en 50 Wbp. Voor een vordering op grond van art. 6:162 BW of 3:296 BW is voorts (de mogelijkheid van) schade een vereiste. De Wbp stelt dit vereiste niet. Er staan het CBP overigens op dit moment nog weinig middelen ter beschikking om het niet-nakomen van een meldplicht jegens de betrokkene te sanctioneren. In het bijzonder kan het CBP geen boete opleggen wegens overtreding van art. 6 Wbp.[23] Hooguit zou het CBP middels bestuursdwang kunnen afdwingen dat de verantwoordelijke de betrokkenen alsnog informeert. Dit wordt anders indien het Consultatievoorstel of de Conceptverordening van kracht worden, nu hierin aanzienlijke boetes zijn opgenomen voor overtreders van de in te voeren meldplichten.[24]

Opgemerkt wordt daarnaast dat bij de invulling van het criterium 'zorgvuldig' mede aansluiting gezocht dient te worden bij het begrip 'eerlijk' of 'fair' zoals dat in art. 6 lid 1 onder a van de Richtlijn Bescherming Persoonsgegevens voorkomt.[25] Het begrip 'zorgvuldig' krijgt in de context van de verwerking van persoonsgegevens een specifieke invulling waarbij in de literatuur eerder art.

---

21 CBP 4 maart 2003, z2002-0230, *Uitsprakenbundel Wet bescherming persoonsgegevens 2009*, nr. 6.4.
22 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 20 en p. 77-78.
23 Een bestuurlijke boete kan het CBP alleen voor overtreding van art. 27, 28 of 79 lid 1 Wbp opleggen (art. 66 Wbp).
24 In het Consultatievoorstel wordt het CBP de bevoegdheid gegeven bij niet-naleven van de meldplicht een boete op te leggen van € 200 000. In de Conceptverordening wordt in art. 79 lid 4 in het algemeen aangegeven dat sancties doeltreffend, evenredig en afschrikwekkend dienen te zijn. Wanneer opzettelijk of uit nalatigheid geen melding bij de toezichthoudende autoriteit of de betrokkene gedaan wordt, legt de toezichthoudende autoriteit een geldboete tot € 1 000 000 of, bij een onderneming, een geldboete van 2% van haar jaarlijkse wereldwijde omzet op.
25 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 77-78.

6 Wbp als 'kapstok' wordt gehanteerd dan art. 6:162 BW.

Overweging 38 bij de Richtlijn Bescherming Persoonsgegevens brengt het begrip 'eerlijk' nadrukkelijk in verband met het recht van een betrokkene om op de hoogte te kunnen zijn van een op hem betrekking hebbende verwerking van persoonsgegevens.

Uit de in paragraaf 4.2 aangehaalde passage uit de parlementaire geschiedenis en de UWV-uitspraak volgt dat art. 6 Wbp in bepaalde gevallen een informatieplicht jegens betrokkene met zich mee kan brengen nadat de verplichtingen ingevolge art. 33 en 34 Wbp zijn uitgewerkt, bijvoorbeeld in geval van ontwikkelingen van zodanige aard, dat zij aan de betrokkene bij de verkrijging hadden moeten worden medegedeeld indien zij op dat tijdstip bekend waren geweest.

4.4 *Art. 6:162 BW*

Art. 6:162 BW geeft betrokkenen een grondslag om schadevergoeding te vorderen in geval van onrechtmatig handelen. Ingevolge art. 3:296 BW kan daarnaast een verbod of een gebod worden gevorderd om een einde te maken aan onrechtmatig handelen of nalaten of om toekomstig onrechtmatig handelen of nalaten te voorkomen dat (mogelijk) schade zal veroorzaken.[26] Na invoering van de meldplichten uit het Consultatievoorstel of de Conceptverordening kunnen dergelijke vorderingen worden gebaseerd op een doen of nalaten in strijd met een wettelijke plicht. Zolang dit niet het geval is zal de vordering gebaseerd dienen te worden op een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, al zou ook kunnen worden betoogd dat het handelen in strijd met deze zorgvuldigheidsnorm mede als een inbreuk op art. 6 Wbp en zodoende als strijdig met een wettelijke plicht moet worden gezien. Voor het resultaat maakt dit niet uit.

Opgemerkt wordt dat meldplichten zich naar hun aard niet lenen voor handhaving middels een verbod of een gebod – op het moment dat de vordering wordt ingesteld zal de mede te delen informatie immers reeds bekend zijn bij degene die de vordering wenst in te stellen. Wel is denkbaar dat bijvoorbeeld een consumentenorganisatie bij een groot datalek een collectieve vordering instelt en als nevenvordering eist dat alle betrokkenen alsnog door de verantwoordelijke worden geïnformeerd (art. 3:305a BW).[27] In veel gevallen zal daarnaast geen sprake zijn van noemenswaardige vermogensschade door het niet-voldoen aan de meldplicht al kan dat anders zijn indien het bij de gelekte gegevens bijvoorbeeld gaat om creditcardgegevens en er middels een tijdige mededeling fraude voorkomen had kunnen worden.

Over de vraag wanneer het nalaten van het melden van een beveiligingsinbreuk of datalek in strijd is met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, bestaat geen specifieke civielrechtelijke jurisprudentie of literatuur. Om deze vraag te beantwoorden kan enerzijds worden aangesloten bij het begrip 'eerlijk' in de Europese richtlijn en de wetsgeschiedenis, literatuur en jurisprudentie bij art. 6 Wbp (ten aanzien waarvan wordt verwezen naar paragraaf 4.3 hierboven), anderzijds bij het algemene kader aangaande informatie- en waarschuwingsplichten onder art. 6:162 BW.

Verplichtingen om te informeren of te waarschuwen – in de vorm van plichten om op straffe van aansprakelijkheid te waarschuwen of voorzorgsmaatregelen te treffen – zijn in dit kader in het bijzonder ontwikkeld rond situaties van gevaarzetting,[28] waarbij de criteria die worden genoemd in het *Kelderluik*-arrest leidend zijn.[29] Een meldplicht op grond van deze jurisprudentie zal voornamelijk aan de orde zijn indien door een datalek gevaar of schade kan ontstaan. Jansen heeft in een recente dissertatie op een rij gezet welke gezichtspunten in zijn visie in het bijzonder van belang zijn om in een aansprakelijkheidscontext een informatieplicht aan te nemen.[30] Afgewogen zal moeten worden of de laedens, gegeven zijn kennis omtrent (i) het betrokken risico, (ii) de dreigende schade en (iii) de potentiële onoplettendheid van het slachtoffer, (iv) naar maatstaven van zorgvuldig-

> Eerder dit jaar werden door het medisch onderzoekscentrum Diagnostiek voor U zeer gevoelige medische gegevens van duizenden Brabanders gelekt. Het ging om medische dossiers van een onderzoekscentrum waarin onder andere te zien was wie HIV-patiënt of alcohol- en drugsverslaafde is. Ook was informatie over het gebruik van medicijnen te vinden. Via een van de websites van het onderzoekscentrum was vrij eenvoudig toegang tot deze gegevens te verkrijgen. De gebruikersnaam voor het systeem bestond uit een vijftal cijfers en het bijbehorende wachtwoord was daaraan identiek en daarom (te) makkelijk te raden.

26 De betrokkene heeft de mogelijkheid om deze vorderingen in te stellen naast de (aanvullende) mogelijkheden die art. 49 en 50 Wbp hem bieden.

27 Bijvoorbeeld door nakoming te vorderen van de meldplicht. Zie mede lid 3 van dit artikel, dat strekt tot een veroordeling tot het openbaar maken van de uitspraak.

28 J.B.M. Vranken, *Mededelings-, informatie- en onderzoeksplichten in het verbintenissenrecht*, Zwolle: W.E.J. Tjeenk Willink 1989, p. 152.

29 HR 5 november 1965, *NJ* 1966, 136.

30 K.J.O. Jansen, *Informatieplichten: over kennis en verantwoordelijkheid in contractenrecht en buitencontractueel aansprakelijkheidsrecht* (diss. Leiden), Deventer: Kluwer 2012.

> Een ander opvallend geval had betrekking op een procederende Telfort-klant. Deze vroeg aan incassobureau GGN een verklaring van schuldovername. Naar aanleiding van dit verzoek kreeg de klant een lijst toegestuurd waarop de naam, het adres, mobiele telefoonnummer, geboortedatum en hoogte van de schuld van 1243 wanbetalers stonden. Een woordvoerder van GGN verklaarde dat het niet mogelijk was de privé-informatie omtrent vorderingen per cliënt apart toe te sturen, aangezien deze allen tezamen in één Excel-bestand staan.

heid was gehouden tot een waarschuwing.[31] Beslissend daarbij is of de laedens meer risico heeft genomen dan redelijkerwijs verantwoord was door de gelaedeerde niet te waarschuwen. De aard van de rechtsverhouding, de aard van de betrokken informatie en de aard van de betrokken belangen kunnen in dit verband dienen als gezichtspunten.[32]

4.5 *Art. 6:248, 7:401, 7:403 en 7:611 BW*

Ook uit een contractuele verhouding tussen verantwoordelijke en betrokkene kan in bepaalde gevallen een meldplicht voortvloeien, in de eerste plaats uiteraard indien partijen een expliciete verplichting op dit punt in hun overeenkomst hebben opgenomen.

Contractuele verhoudingen worden daarnaast beheerst door de redelijkheid en billijkheid. Partijen dienen hun gedrag mede te laten bepalen door de gerechtvaardigde belangen van hun contractuele wederpartij.[33] Ingevolge art. 6:248 lid 1 BW kunnen uit de redelijkheid en billijkheid, in het licht van de aard van de overeenkomst, aanvullende verplichtingen voor contractspartijen voortvloeien. Hieronder kunnen ook informatieplichten vallen.[34] Indien de verwerking van persoonsgegevens plaatsvindt in het kader van een overeenkomst van opdracht tussen de betrokkene en de verantwoordelijke kan een verplichting tot melden van beveiligingsinbreuken of datalekken volgen uit art. 7:401 of art. 7:403 BW, bij een arbeidsovereenkomst uit art. 7:611 BW. De genoemde artikelen zijn een uitwerking van de redelijkheid en billijkheid en de daaruit voortvloeiende op de opdrachtnemer althans de werkgever rustende zorgplicht.

De verplichtingen die voortvloeien uit art. 6:248, 7:401, 7:403 en 7:611 BW worden nader ingekleurd door de verplichtingen uit de Wbp, waaronder art. 6 Wbp.[35] Het niet-naleven van de verplichtingen uit de Wbp zal, indien de belangen van de betrokkene hierdoor worden geraakt, in veel gevallen een tekortschieten opleveren onder de overeenkomst, ook indien naleving van deze verplichtingen niet expliciet is overeengekomen.

Schending van een contractuele meldplicht kan onder omstandigheden – naast de mogelijkheid van het vorderen van schadevergoeding – aanspraak geven op ontbinding van de overeenkomst.

4.6 *Toepassing*

In de voorgaande paragrafen zijn vanuit het privacyrecht en het privaatrecht diverse gezichtspunten geschetst aangaande mogelijke meldplichten van de verantwoordelijke jegens de betrokkene naar aanleiding van datalekken. Het is nu tijd om tot een synthese van deze gezichtspunten te komen.

Bij de verschillende grondslagen die wij hebben besproken gaat het om open zorgvuldigheidsnormen, die afhankelijk van de omstandigheden van het geval kunnen meebrengen dat er op de verantwoordelijke een meldplicht jegens de betrokkene rust. Deze meldplicht vloeit voort uit de zorg die zowel ingevolge art. 6 Wbp en art. 6:162 BW als ingevolge art. 6:248, 7:401 en 7:611 BW rust op de verantwoordelijke.

Als wordt gekeken vanuit de privacyrechtelijke invalshoek speelt het transparantiebeginsel een grote rol. Het beginsel van een eerlijke gegevensverwerking eist dat de betrokkene op de hoogte kan zijn van een op hem betrekking hebbende gegevensverwerking. Nieuwe ontwikkelingen van zodanige aard dat zij aan de betrokkene bij de verkrijging hadden moeten worden medegedeeld indien zij op dat tijdstip bekend waren geweest, kunnen aanleiding geven tot een verplichting tot aanvullende informatieverstrekking. Een datalek zal in veel gevallen als een zodanige ontwikkeling gekwalificeerd moeten worden.

Ter relativering merken wij overigens op dat wij in een beperkt onderzoek in de internationale literatuur weinig bevestiging voor dit standpunt hebben gevonden. Voor zover ons bekend is buiten Nederland alleen in Denemarken gesignaleerd dat een dergelijke verplichting volgt uit het beginsel van een eerlijke gegevensverwerking.[36]

---

31 Jansen 2012, *supra* noot 30, p. 387 e.v.
32 Jansen 2012, *supra* noot 30, p. 429.
33 Zie HR 15 november 1957, *NJ* 1958, 67 (*Baris/Riezenkamp*) en Asser/Hartkamp & Sieburgh 2010 (6-III*), nr. 392.
34 Jansen 2012, *supra* noot 30, p. 256.
35 Zie m.b.t. art. 6:248 lid 1 BW en publiekrechtelijke regels uit het financiële toezichtrecht de noot van M.R. Mok onder HR 23 december 2005, *NJ* 2006, 289, par. 2: 'Op grond van art. [6; JB en MvR]:248, lid 1, BW kan men echter aannemen dat de publiekrechtelijke verplichtingen van een financiële dienstverlener in de contractuele verhouding tussen die dienstverlener en haar cliënten wordt gereflecteerd'.
36 Vgl. in dit verband mede Kuner 2007, *supra* noot 19, die wel ingaat op de vraag of dit volgt uit art. 10 van de richtlijn en op het doelbindingscriterium van art. 6, maar niet op *fair processing*. Vgl. tevens de landenrapporten op de website van Linklaters (https://clientsites.

Bezien vanuit het leerstuk van de onrechtmatige daad vereist de zorgvuldigheid een waarschuwing indien een bij de verantwoordelijke bekend risico, met het oog op dreigende schade en potentiële onoplettendheid van de betrokkene, daar naar maatstaven van zorgvuldigheid aanleiding toe geeft. Daarbij spelen de aard van de rechtsverhouding, de aard van de betrokken informatie en de aard van de betrokken belangen als gezichtspunten een rol. Bij de verwerking van persoonsgegevens wijzen deze gezichtspunten in onze visie in de richting van het aannemen van een waarschuwingsplicht indien er (waarschijnlijk) persoonsgegevens zijn gelekt en belangen van de betrokkene hierdoor (mogelijk) worden geschaad, gezien de zorgplicht die ingevolge art. 6 Wbp op de verantwoordelijke rust en de aard van de privacybelangen die (naast eventuele te lijden vermogensschade) mogelijk worden geschonden. Een betrokkene zal (en mag) er daarnaast over het algemeen van uitgaan dat zijn persoonsgegevens veilig zijn bij de verantwoordelijke. Hij zal dan ook in beginsel niet verdacht zijn op het lekken van zijn gegevens en van hem hoeft in principe geen grote oplettendheid verwacht te worden. Vgl. in dit verband tevens de eerdergenoemde UWV-uitspraak waarin voor het aannemen van een informatieplicht doorslaggevend was dat afgeweken werd van wat betrokkene redelijkerwijs kon verwachten.

In een contractuele context kan een meldplicht, mede afhankelijk van de inhoud en aard van de overeenkomst, aanvullend voortvloeien uit art. 6:248, 7:401, 7:403 en 7:611 BW.

Gecombineerd brengen deze perspectieven ons tot de conclusie dat een datalek dat nadelige gevolgen voor de betrokkene kan veroorzaken nu reeds in veel gevallen door de verantwoordelijke aan de betrokkene zal moeten worden gemeld. Bij de vraag of deze verplichting in een concreet geval bestaat spelen onder meer de volgende omstandigheden een rol:

a. De aard en gevoeligheid van de gelekte gegevens. Vgl. in dit verband andermaal de UWV-uitspraak, waar het ging om bijzondere persoonsgegevens. De gevoelige aard van deze gegevens was in dit geval een indicatie voor het aannemen van een informatieplicht. Bij de vraag of de aard of gevoeligheid van de gegevens een indicatie is om te melden kan daarnaast bijvoorbeeld de vraag een rol spelen of de gegevens reeds openbaar waren. Het lekken van telefoonnummers die ook in het telefoonboek staan zal niet snel aanleiding geven tot een meldplicht, het lekken van geheime nummers veeleer wel.

b. De aard van het bedrijf of de organisatie van de verantwoordelijke.[37]

c. De aard en het doel van de oorspronkelijke verwerking.

d. De aard van de relatie tussen de verantwoordelijke en de betrokkene (contractueel of niet contractueel, beschermingskarakter zoals bijvoorbeeld aan de orde in een overeenkomst met een werknemer of consument).[38]

e. De mogelijke schade die uit het niet-melden kan voorvloeien voor de betrokkene.

f. De vraag of de betrokkene nog iets kan doen om dergelijke schade te beperken, zoals bijvoorbeeld het blokkeren van een creditcard, wijzigen van een wachtwoord of het wijzigen van een telefoonnummer.

g. De mate van verspreiding van de gelekte gegevens. Het is bijvoorbeeld voorstelbaar dat bij een 'hack' de dader al is gepakt en vaststaat dat de gegevens niet zijn verspreid, of dat de 'hacker' uit idealistische motieven heeft gehandeld om een ondeugdelijke beveiliging als misstand aan de kaak te stellen en vaststaat dat de gegevens niet zijn gekopieerd of vrijwillig zijn vernietigd. Melding aan de betrokkene lijkt dan minder urgent.

h. De vraag of encryptie is toegepast op de gegevens. Indien de gelekte persoonsgegevens via encryptie voldoende deugdelijk ontoegankelijk zijn gemaakt zou van melding afgezien kunnen worden.[39]

i. De inspanning die het kost om de betrokkene de bereiken.[40]

j. De vraag of het datalek in de openbaarheid is gekomen (zodat de betrokkene mogelijk al op de hoogte is).[41]

k. De vraag of het datalek aan de toezichthoudende autoriteiten en/of de politie is gemeld.

l. De onrust of juist de 'afstompende werking'[42] die het bekendmaken van het datalek kan veroorzaken.

m. De verwijtbaarheid van het datalek.

5 Afronding

De conclusie op basis van het voorgaande is dat er – buiten sectorwetgeving (telecom, financiële sector) en een zeer beperkte strafrechtelijke aangifteverplichting – geen verplichting rust op een verantwoordelijke om het bevoegd gezag op de hoogte te stellen van beveiligingsin-

linklaters.com/Clients/dataprotected/Pages/index.aspx) waarin alleen in de Nederlandse en de Deense bijdrage een verplichting wordt gesignaleerd gebaseerd op 'fair processing'. P. Carey, *Data Protection; A Practical Guide to UK and EU Law*, New York: OUP 2009, p. 101 stelt expliciet dat er geen verplichting bestaat.

37 Vgl. in dit verband p. 9 van de toelichting bij het Consultatievoorstel, waar wordt overwogen dat het hacken van de ledenadministratie van een sportvereniging niet tot een melding bij het CBP (en hiermee samenhangende een melding aan de betrokkenen) hoeft te leiden nu de gevolgen van een dergelijk datalek doorgaans beperkt blijven en ook van betrokkenen kan worden gevergd dat zij een zekere mate van risico aanvaarden. Dit is volgens de toelichting anders in geval van een datalek bij de belastingdienst of een bank.

38 In de UWV-uitspraak werd benadrukt dat de betrokkene ten opzichte van het UWV in een afhankelijke positie verkeerde.

39 Vgl. lid 6 van het nog in te voeren art. 34a Wbp.

40 Vgl. art. 34 lid 4 Wbp – onevenredige inspanning.

41 Vgl. art. 33 lid 1 en 34 lid 1 Wbp: 'tenzij deze reeds daarvan op de hoogte is'.

42 Vgl. P. Kuipers, 'Aansprakelijkheid voor "terughaalschade" en waarschuwingsplichten van de producent bij (mogelijke) product recall', *AV&S* 2001, par. 2.3.

breuken en datalekken. Dit wordt in de toekomst waarschijnlijk anders nu er diverse initiatieven aanhangig zijn om dergelijke verplichtingen te creëren, tezamen met verplichtingen om aan de betrokkene te melden.

Tussen een verwerker en een verantwoordelijke, en de verantwoordelijke en derden, kan een verplichting volgen uit de contractuele relatie. Het is verstandig om in een bewerkersovereenkomst en in andere overeenkomsten die betrekking hebben op de verwerking van persoonsgegevens duidelijke afspraken te maken over de gevallen waarin melding gemaakt dient te worden van beveiligingsinbreuken en datalekken, al dan niet versterkt door een boete. De Conceptverordening gaat uit van de verplichting van de bewerker om een datalek aan de verantwoordelijke te melden.

De verantwoordelijke is onder het huidige wettelijke regime in onze optiek, afhankelijk van de omstandigheden, in veel gevallen reeds gehouden om datalekken te melden aan de betrokkene. Zolang deze verplichting is gebaseerd op de algemene zorgvuldigheidsnormen uit art. 6 Wbp en het Burgerlijk Wetboek kan deze verplichting afhankelijk van de relevante omstandigheden voldoende flexibel worden gehanteerd. Dat maakt de invoering van een specifieke wettelijke regeling overigens niet overbodig. De handhaafbaarheid en de rechtsbescherming van betrokkenen kan hierdoor immers worden vergroot.

De rechtspositie van ondernemingen wordt met de huidige voorstellen, waarin de meldplicht aan zowel het bevoegd gezag als aan betrokkenen afhangt van de invulling van open normen en er tevens forse boetes worden verbeurd indien niet aan de verplichtingen wordt voldaan, echter onzekerder. In de toelichting op het Consultatievoorstel wordt gesuggereerd dat de meldplicht in veel gevallen niet van toepassing zal zijn.[43] De open normen bieden echter onvoldoende houvast om in een concreet geval met zekerheid vast te kunnen stellen dat van melding afgezien kan worden. Van het CBP en/of de toekomstige European Data Protection Board mag worden verwacht dat in richtsnoeren nader wordt uitgewerkt in welke gevallen melding is vereist[44] en in (boete)beleidsregels hoe overtreding zal worden gesanctioneerd. Het lijkt na invoering van de beoogde meldplichten voorlopig verstandig om bij de geringste twijfel zekerheidshalve tenminste aan het bevoegd gezag te melden, in ieder geval totdat middels richtsnoeren en beleidsregels nader verduidelijkt is in welke gevallen gemeld dient te worden en hoe met de in te voeren sanctiebevoegdheden omgegaan zal worden.

Het meest recente grote datalek was eind augustus bij de website www.tix.nl. Een hacker van het Nederlands Genootschap van Hackende Huisvrouwen ontdekte dat door een fout in de software van de website ruim 2600 persoonlijke documenten online stonden via een onbeveiligde internettoegang. Tussen de bestanden zaten zeer privacygevoelige documenten, namelijk kopieën van paspoorten, financiële gegevens (bankafschriften, afbeeldingen van creditcards met zowel de voorkant als de achterkant met een vertrouwelijke code), medische informatie van reizigers, een overlijdensakte en diverse brieven van de Duitse politie. De webserver waar deze documenten op stonden was volledig voor het publiek toegankelijk.

43 Zie p. 8 van de toelichting bij het Consultatievoorstel onder het kopje 'Voorkomen van nodeloze meldingen'.
44 De toelichting bij het Consultatievoorstel, p. 8, verwijst in dit verband naar voorlichtende maatregelen van het CBP.