NOREA
de beroepsorganisatie van IT-auditors

Staatssecretaris F. Teeven,
Veiligheid en Jusititie,
Postbus 20301
2500 EH DEN HAAG

Onze ref : AB/wo/2012-43
Doorkiesnr. : 020-3010385 / Faxnummer: 020-3010302
Datum : 29-02-2012
Betreft : Reactie NOREA op internetconsultatie gebruik camerabeelden en meldplicht datalekken

Geachte heer Teeven,

Internetconsultatie Wijziging Wbp
NOREA, de beroepsorganisatie van IT-auditors, maakt graag gebruik van de geboden gelegenheid om te reageren op het concept wetsvoorstel Wijziging Wbp, waarin ook een regeling is opgenomen voor een meldplicht voor datalekken.

Beoordelingscriteria
NOREA heeft het concept wetsvoorstel voor wat betreft de meldplicht datalekken beoordeeld vanuit de invalshoek of daarmee een bijdrage wordt geleverd aan de door het kabinet geformuleerde doelstelling, namelijk dat de meldplicht "*bijdraagt aan een grotere transparantie bij de verwerking van persoonsgegevens, ruimere aandacht voor de noodzaak goed te investeren in beveiligingsmaatregelen, en op den duur toename van het vertrouwen van de samenleving in de geautomatiseerde verwerking van persoonsgegevens*". In dat kader heeft NOREA mede beoordeeld of het wetsvoorstel in voldoende mate de controleerbaarheid van de invulling van de meldplicht ondersteunt. Dat zou het behalen van de doelstelling verder bevorderen.

Algemene conclusie:
In een brief aan de Eerste Kamer, gedateerd op 28 april 2011, heeft NOREA gepleit voor het afdwingen van effectieve (zelf)regulering door verwerkers van persoonsgegevens en het realiseren van een robuuster extern toezicht door het College bescherming persoonsgegevens (CBP). NOREA is van mening dat de meldplicht datalekken mede (deels) invulling geeft aan dat pleidooi. Immers, de meldplicht zal verwerkers van persoonsgegevens meer bewust maken van het belang van een effectieve bescherming van de persoonlijke levenssfeer. Dit bewustzijn zal tot gevolg hebben dat de toepassingscultuur zal verbeteren alsmede dat meer en beter verantwoording aan het maatschappelijk verkeer zal worden afgelegd. En dat is een goede zaak!

NOREA pleit in deze brief voor een aantal (aanvullende) maatregelen ten aanzien van de meldplicht datalekken om de effecten daarvan op de doelstelling alsmede op de integriteit en de controleerbaarheid van de meldplicht verder te verbeteren. Deze maatregelen zijn er met name op gericht om het "level playing field" dat zo noodzakelijk is om te voorkomen dat "de goeden onder de slechten lijden" te waarborgen.

Reikwijdte van de meldplicht: voor evenwichtige toepassing is verdere uitwerking van het beslismodel noodzakelijk

Het kabinet heeft er bewust voor gekozen om nodeloze meldingen te voorkomen. NOREA is het hier mee eens. Als gevolg daarvan is het noodzakelijk dat normen worden ontwikkeld die de noodzakelijke en de nodeloze meldingen van elkaar onderscheiden.

De reikwijdte van de meldplicht wordt (vooral) in artikel 34a lid 1 gedefinieerd. Daarbij worden de volgende termen gehanteerd: “redelijkerwijs”, “aangenomen”, “aanmerkelijk risico”, “nadelige gevolgen”. Deze termen dienen stuk voor stuk te worden geïnterpreteerd om te bepalen of aan de meldplicht invulling moet worden gegeven. In de Memorie van Toelichting is in paragraaf 4.1.4 een beslismodel voor de verantwoordelijke beschreven. Dit beslismodel laat nog te veel ruimte voor sterke interpretatieverschillen.

Voorstel aanvullende maatregel: NOREA acht het noodzakelijk dat het beslismodel nader wordt uitgewerkt om te voorkomen dat door verantwoordelijken op volstrekt onevenwichtige wijze aan de meldplicht invulling wordt gegeven. Wij kunnen ons voorstellen dat een dergelijke uitwerking door het CBP zal plaatsvinden.

Controleerbaarheid van de meldplicht: voor een verdere druk op het daadwerkelijk invullen van de meldplicht is een jaarlijkse bestuursverklaring over datalekken voor bepaalde gevoelige verwerkingen noodzakelijk

Om de meldplicht datalekken evenwichtig te laten functioneren is het noodzakelijk dat organisaties die welbewust de meldplicht “aan hun laars lappen” met een hoge waarschijnlijkheid daarmee worden geconfronteerd. Dit kan geschieden door verschillende personen en instanties, waaronder (externe) auditors en accountants, toezichthouders (bijv. CBP) en de pers. NOREA acht het echter onwaarschijnlijk dat de meldplicht datalekken zoals die nu is opgesteld leidt tot een hoge pakkans. Het stilhouden van datalekken vanwege de reputatieschade die daaruit kan voortvloeien is dan een verleidelijk scenario. Wel is NOREA in dit kader verheugd over het hoge maximale boetebedrag ad. € 200.000 dat voor verzuim van de meldplicht wordt ingesteld.

Voorstel aanvullende maatregel: NOREA acht het noodzakelijk dat – bijvoorbeeld voor verwerkingen van (impliciet) gevoelige gegevens danwel voor verwerkingen vanaf risicocategorie II[1]– het bestuur van de organisatie van de verantwoordelijke jaarlijks expliciet verklaart dat geen datalekken zijn vastgesteld en deze verklaring aan het CBP ter beschikking stelt.

[1] Zie hoofdstuk 3.3 van “Beveiliging van persoonsgegevens”, Achtergrondstudies en Verkenningen 23, CBP, april 2001 (http://www.cbpweb.nl/downloads_av/av23.pdf).

NOREA
de beroepsorganisatie van IT-auditors

Inbreuk op de beveiligingsmaatregelen: reikwijdte onduidelijk van 'inbreuk op de maatregelen, bedoeld in artikel 13 [Wbp]'. Geen maatregelen, geen meldplicht?
Op grond van het voorgesteld artikel 34a Wbp dient de verantwoordelijke iedere inbreuk op de maatregelen die zijn genomen (op grond van artikel 13 Wbp) om persoonsgegevens te beveiligen te melden. Opvallend hierbij is dat dus niet iedere inbreuk gemeld dient te worden. Dit volgt letterlijk uit de tekst van het voorstel:

> *Er is pas sprake van een datalek, wanneer die technische en organisatorische maatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijk risico van verlies of onrechtmatige verwerking.*

`Hierbij wordt er van uit gegaan dat er überhaupt beveiligingsmaatregelen zijn genomen. De vraag is echter of deze aanname wel realistisch is. Talrijke voorbeelden zijn te noemen waaruit blijkt dat persoonsgegevens soms helemaal niet worden beveiligd.[2]

Dit kan tot de merkwaardige situatie leiden dat organisaties die geen maatregelen conform artikel 13 Wbp hebben getroffen *niet* verplicht is tot het melden van een datalek. Hoewel daarmee hoogstwaarschijnlijk artikel 13 Wbp wordt geschonden, wordt het nalatend handelen van de organisatie beloond. Immers, schending van artikel 13 Wbp levert geen (financiële) sanctie op en schending van het voorgesteld artikel 34a Wbp kan een sanctie tot 200.000 betekenen.

De organisaties die wel de moeite hebben genomen om beveiligingsmaatregelen te treffen, zijn echter wel gedwongen een melding te doen bij het College Bescherming Persoonsgegevens. Bovendien kan niet nalaten of niet tijdig voldoen van de melding een boete van maximaal 200.000 opleveren.

Zowel externe als interne onrechtmatige verwerkingen: Niet geheel duidelijk is geworden hoe ver de definitie 'inbreuk op maatregelen' strekt.
Voor de hand ligt natuurlijk een hackersaanval dat de beveiliging van een database heeft weten te omzeilen en daarmee inbreuk heeft weten te maken op de (beveiligings-)maatregelen van de organisatie.

Het is echter ook mogelijk dat er intern inbreuken plaatsvinden door bijvoorbeeld een van de medewerkers. Denk aan de receptionist die onrechtmatige persoonsgegevens verstrekt aan onbevoegden of een brief verkeerd adresseert. Dienen deze interne onrechtmatige verwerkingen tevens te worden gemeld bij het College Bescherming Persoonsgegevens?

> *Het beveiligingsvoorschrift richt zich tegen 'verlies of enige vorm van onrechtmatige verwerking van gegevens'. Onder onrechtmatige vormen van verwerking vallen de aantasting van gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking.*

In hoeverre wordt er aangesloten bij de definitie zoals deze is vastgelegd in artikel 11.1 sub j van de Telecommunicatiewet?

> *'een inbreuk op de beveiliging die resulteert in een onbedoelde of onwettige vernietiging, verlies, wijziging, niet geautoriseerde toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.'*

ENISA, de European Network and Information Security Agency, heeft onder meer achttien bevoegde nationale instanties geïnterviewd om een beeld te krijgen van waar zij aan denken bij datalekken. De instanties blijken veel situaties als datalekken te beschouwen die niet direct te

[2] Zie bijvoorbeeld https://www.bof.nl/category/zwartboek-datalekken/

maken hebben met de beveiliging van de communicatiedienst of het netwerk zelf. Zo wordt de situatie genoemd waarin een aanbieder een laptop of een USB-stick met persoonsgegevens kwijtraakt. Andere genoemde voorbeelden zijn het verkeerd adresseren van een brief of e-mail die persoonsgegevens bevat en het bij het vuilnis zetten van gevoelige dossiers. Eén toezichthouder noemt ook het gebruik van persoonsgegevens voor direct marketing zonder toestemming van de betrokkene als voorbeeld van een datalek.[3]

Voorstel aanvullende maatregel: NOREA acht het noodzakelijk meer duidelijkheid te verschaffen omtrent het in het eerste lid van het conceptvoorstel genoemde 'inbreuk op maatregelen, bedoeld in artikel 13'. Wenselijk is de meldplicht niet te koppelen aan het feit of er maatregelen conform artikel 13 Wbp zijn genomen of niet. Tevens helderheid te verschaffen omtrent de vraag of zowel interne als externe onrechtmatige verwerkingen gemeld dienen te worden.

Zowel melding aan CBP als aan betrokkene:
Volgens het voorstel moet de melding onverwijld zowel aan de CBP als de betrokkene wiens gegevens mogelijk door ene inbreuk zijn getroffen worden gedaan.
Zowel het CBP als de betrokkene dienen 'onverwijld' op de hoogte te worden gehouden van de inbreuk waardoor het lijkt dat beide tegelijkertijd, of in ieder geval kort na elkaar op de hoogte dienen te worden gehouden. Dit lijkt echter in conflict te staan met het zesde lid uit het voorgestelde artikel 34a Wbp:

> *'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*'.

Het lijkt erop dat de verantwoordelijke allereerst toestemming aan het College dient te vragen om de melding aan de betrokkene achterwege te laten. Van het 'onverwijld' de betrokkene op de hoogte houden lijkt dan geen sprake meer.

Of is de bedoeling van het voorstel dat de verantwoordelijke in eerste instantie eerst bij het CBP de melding verricht en zelf de afweging dient te maken of het nodig is tevens een melding te doen bij de betrokkene. Dit bijvoorbeeld in het geval van de in het voorstel genoemde encryptie van de data. Op grond van artikel 7 kan het CBP alsnog de verantwoordelijke bevelen de inbreuk aan de betrokkene te melden.

Voorstel aanvullende maatregel: NOREA acht het noodzakelijk meer duidelijkheid te verschaffen omtrent de vraag of het College of de verantwoordelijke de afweging dient te maken of 'gepaste maatregelen' zijn genomen.

met vriendelijke groet,
namens het Bestuur,

i/o

mr.drs. J. Roodnat RE RA,
Secretaris

[3] Mr. F.J. Zuiderveen Borgesius, 'De meldplicht voor datalekken in de Telecommunicatiewet', Computerrecht aug 2011, p. 212.

Postbus 7984
1008 AD AMSTERDAM
020-3010380
www.norea.nl
norea@norea.nl