



0 BD



POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10  
 TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpreweb.nl www.mijnprivacy.nl

02/21/2014

AAN Staatssecretaris van Veiligheid en Justitie  
 De heer mr. F. Teeven  
 Postbus 20301  
 2500 EH Den Haag

DATUM 20 februari 2014

ONS KENMERK

CONTACTPERSOON

UW BRIEF VAN

UW KENMERK

12:11:001

ONDERWERP Wetsvoorstel meldplicht datalekken

Geachte heer Teeven,

Op 10 februari 2014 hebben wij bestuurlijk overleg gevoerd over – onder meer – het wetsvoorstel meldplicht datalekken. In dit overleg heeft het College bescherming persoonsgegevens (CBP) zijn bezwaren geuit tegen de voornemens die uw ministerie te kennen heeft gegeven om het wetsvoorstel te wijzigen. In deze brief licht ik deze bezwaren graag toe aan de hand van de concept-nota van wijziging die het CBP op 10 februari 2014 van het ministerie van Veiligheid en Justitie ontving.

In het regeerakkoord 'Vrijheid en verantwoordelijkheid' uit 2010 kondigde het toenmalige kabinet aan met een voorstel te zullen komen "voor een meldplicht voor alle diensten van de informatiemaatschappij, waaronder de overheid, in geval van verlies, diefstal of misbruik van persoonsgegevens waarbij *alle datalekken* [cursivering CBP] worden gemeld aan de nationale toezichthouder die boetes kan opleggen indien de meldplicht niet wordt nageleefd." In de memorie van toelichting bij het wetsvoorstel refereert u expliciet aan dit voornemen.<sup>1</sup> Het CBP is altijd een warm voorstander van de meldplicht geweest aangezien deze de bescherming van persoonsgegevens in het algemeen, en de versterking van de positie van de burger in het bijzonder in hoge mate kan dienen. De beoogde effecten zullen echter uitsluitend worden bereikt als de wettelijke meldplicht op een daartoe passende wijze is vormgegeven.

In de concept-nota van wijziging van 10 februari 2014 wordt voorgesteld om de omschrijving van de reikwijdte van de meldplicht in het eerste lid van het nieuwe artikel 34a Wbp aan te passen, en om vervolgens door aanpassing van het zesde lid van dit artikel de reikwijdte van de meldplicht sterk in te perken.

De wettelijke drempel voor het melden van inbreuken wordt door de voorgestelde aanpassingen dermate hoog dat in de praktijk alleen nog de datalekken zullen worden gemeld waarvan de ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens volstrekt evident zijn. In combinatie met de voorgestelde aanpassing in het vierde lid van artikel 34a Wbp

<sup>1</sup> Kamerstukken II 2012-13, 33662, 3, p. 2.

DATUM 20 februari 2014  
ONS KENMERK

02/21/2014

leiden deze aanpassingen er verder toe dat verantwoordelijken inbreuken pas zullen melden op het moment dat zich daadwerkelijke ernstige nadelige gevolgen hebben voorgedaan.

De melding krijgt daarmee het karakter van de put die wordt gedempt wanneer het kalf reeds verdronken is; na de zelf-incriminatie van de verantwoordelijke rest de toezichthouder slechts de mogelijkheid tot repressief optreden. De preventieve rol die voor de toezichthouder in het oorspronkelijk ingediende wetsvoorstel nog was weggelegd is in de nota van wijziging geheel verdwenen.

Naar het oordeel van het CBP gaan de voorgestelde aanpassingen aanzienlijk verder dan nodig is om meldingen van bagatelzaken tegen te gaan. In het verslag van de vaste commissie voor Veiligheid en Justitie d.d. 9 september 2013 ziet het CBP geen aanleiding voor de ingrijpende aanpassingen die in de nota van wijziging van 10 februari 2014 worden voorgesteld. Ook zijn de voorgestelde wijzigingen niet in lijn met de meldplicht zoals die is vormgegeven in de voorstellen van de Europese Commissie voor de herziening van het Europese wettelijke gegevensbeschermingskader.

Gezien het bovenstaande geef ik u dringend in overweging om de nota van wijziging niet aldus in te dienen.

Mocht u hierover van gedachten willen wisselen, dan is het CBP daar uiteraard toe bereid.

Hoogachtend,  
Het College bescherming persoonsgegevens,

  
Mr. J. Kobusstamm  
Voorzitter

DATUM 20 februari 2014  
ONS KENMERK

**Wetsvoorstel meldplicht datalekken:  
Commentaar CBP op de concept-nota van wijziging van 10 februari  
2014**

Nadere toelichting per lid van artikel 34a Wbp

Onderstaand worden de bezwaren van het CBP per lid van artikel 34a Wbp nader toegelicht.

Tekst wetsvoorstel	Tekst op basis van nota van wijziging
1. De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens die door hem worden verwerkt.	1. De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die ernstige nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens.

De nieuwe formulering werpt een hogere drempel op voor melding aan de toezichthouder: het is niet meer voldoende dat "redelijkerwijs kan worden aangenomen dat [de inbreuk] leidt tot een aanmerkelijke kans op nadelige gevolgen", maar het moet gaan om een inbreuk "die ernstige nadelige gevolgen heeft".

De nieuwe formulering creëert het risico dat inbreuken pas aan de toezichthouder en aan de betrokkenen worden gemeld op het moment dat de ernstige gevolgen (zoals publicatie van gelekte persoonsgegevens op een hackersite of identiteitsfraude) zich daadwerkelijk hebben voorgedaan. Een groot deel van de toegevoegde waarde van de meldplicht gaat op die manier verloren.

Tekst wetsvoorstel	Tekst op basis van nota van wijziging
4. De kennisgeving aan het College omvat tevens 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.	4. De kennisgeving aan het College omvat tevens een beschrijving van de gevolgen voor de verwerkte persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

De nieuwe formulering wekt de indruk dat uitsluitend nog de geconstateerde gevolgen van de inbreuk in de kennisgeving aan het College hoeven te worden opgenomen, en niet meer de vermoedelijke gevolgen. Het risico dat inbreuken pas aan de toezichthouder en aan de betrokkenen worden gemeld op het moment dat zich daadwerkelijk ernstige gevolgen hebben voorgedaan wordt daardoor vergroot.

Verder is het voor de bescherming van de verwerkte persoonsgegevens van essentieel belang dat verantwoordelijken na een inbreuk vaststellen tot welke gevolgen deze kan leiden en waar

DATUM 20 februari 2014  
ONS KENMERK

mogelijk maatregelen treffen om de betrokkenen tegen deze gevolgen te beschermen. De nieuwe formulering gaat hier volledig aan voorbij.

Tekst wetsvoorstel	Tekst op basis van nota van wijziging
6. De kennisgeving aan de betrokkene is niet vereist indien de verantwoordelijke 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.	6. Het eerste en tweede lid zijn in ieder geval niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk en ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.

Door de nieuwe formulering wordt de meldplicht aan de toezichthouder ingeperkt: als voldaan wordt aan de in lid 6 gestelde voorwaarden – wat in eerste instantie ter beoordeling is aan de verantwoordelijke zelf – vervalt niet alleen de meldplicht aan betrokkene, maar ook de meldplicht aan de toezichthouder. Dit betekent dat de toezichthouder niet meer in de gelegenheid wordt gesteld om te beoordelen of de getroffen technische beschermingsmaatregelen afdoende zijn. Door de nieuwe formulering ontstaat er ook een verschil met de meldplicht in de Tw: onder de 'smalle' meldplicht moeten alle datalekken aan de toezichthouder worden gemeld, en geldt er in de hier bedoelde gevallen alleen een uitzondering op de meldplicht aan de betrokkene.

De stand van de techniek ontwikkelt zich voortdurend, en eenmaal geleepte persoonsgegevens kunnen door toepassing van de nieuwste technologische middelen alsnog begrijpelijk en toegankelijk worden. Nog afgezien daarvan leert de ervaring dat verantwoordelijken lang niet altijd een realistisch beeld hebben van de mate waarin technische beschermingsmaatregelen de verwerkte persoonsgegevens daadwerkelijk onbegrijpelijk en ontoegankelijk maken voor eenieder die geen recht heeft op kennisname. De nieuwe formulering van het zesde lid leidt daarom tot een reëel risico dat inbreuken met ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens noch aan de toezichthouder, noch aan de betrokkene worden gemeld.

Tekst wetsvoorstel	Tekst op basis van nota van wijziging
8. 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.	[Lid vervalt.]

Het vervallen van de wettelijke verplichting tot het bijhouden van een overzicht van alle inbreuken maakt het voor het CBP moeilijker om inzicht te krijgen in de niet gemelde datalekken. Ook de stimulans voor verantwoordelijken om alert te zijn op inbreuken en zich rekenschap te geven van de gevolgen die deze kunnen hebben voor de persoonlijke levenssfeer van de betrokkenen verdwijnt op deze manier.

DATUM 20 februari 2014  
ONS KENMERK

02/21/2014 12:05

Overige opmerkingen

In aanvulling op het bovenstaand wijst het CBP u nog op het volgende. In het wetsvoorstel geldt voor de bestuurlijke boete die het CBP kan opleggen voor de overtreding van de meldplicht een maximum van 450.000 euro. V&J heeft toegelicht waarom daar in het onderhavige wetsvoorstel voor is gekozen. Het CBP gaat er zoals besproken wel van uit dat, bij de uitbreiding van de boetebevoegdheden van het CBP, dit maximum in lijn zal worden gebracht met de overige boetebevoegdheden van het CBP.