**Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken)**

**NOTA VAN WIJZIGING**

Het voorstel van wet wordt gewijzigd als volgt:

A
In artikel I, onderdeel A, wordt in de onderdelen 1, 2 en 4 de zinsnede "waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de persoonsgegevens" vervangen door: die ernstige nadelige gevolgen heeft voor de bescherming van de persoonsgegevens.

B
Artikel I, onderdeel B, wordt gewijzigd als volgt:

1. Voor de tekst van onderdeel B wordt een "2" geplaatst.

2. Een onderdeel 1 wordt toegevoegd, luidende:

1. Aan het opschrift van hoofdstuk 5 wordt toegevoegd "en de meldplicht bij inbreuken op de beveiliging van persoonsgegevens aan het College"

3. In onderdeel 2 (nieuw) wordt artikel 34a gewijzigd als volgt:

a. Het eerste lid komt te luiden:
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.

b. In het vierde lid wordt de zinsnede "de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens" vervangen door: de gevolgen van de inbreuk voor de verwerkte persoonsgegevens.

c. Het zesde lid komt te luiden:
6. Het eerste en tweede lid zijn niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.

d. In het zevende lid wordt "nadelige" vervangen door: ongunstige.

e. Onder vernummering van het negende, tiende en elfde lid tot achtste, negende en tiende lid, vervalt het achtste lid (oud).

C
Artikel I, onderdeel C, wordt gewijzigd als volgt:

1. In het eerste lid van artikel 51a vervalt de zinsnede "op de naleving".

2. Het tweede lid komt te luiden:
2. Het College en de toezichthouders, bedoeld in het eerste lid, zijn bevoegd uit eigen beweging en desgevraagd verplicht aan elkaar de gegevens betreffende de verwerking

van persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van hun taak.
3. Het derde en vierde lid vervallen.

D
Aan artikel I wordt een onderdeel F toegevoegd:

F
In artikel 43 wordt na artikel 34 ingevoegd: , artikel 34a, tweede lid,.

E
Na artikel II wordt een artikel toegevoegd, luidende:

**Artikel IIa**

Indien het bij koninklijke boodschap van 26 april 2013 ingediende voorstel van wet tot wijziging van de Instellingswet Autoriteit Consument en Markt en enige andere wetten in verband met de stroomlijning van het door de Autoriteit Consument en Markt te houden markttoezicht (Kamerstukken 33622) tot wet wordt verheven en artikel XIV van die wet op een eerder tijdstip in werking treedt dan artikel II van deze wet, komen de artikelen II en III te luiden:

**Artikel II**

De Telecommunicatiewet wordt gewijzigd als volgt:

A

In artikel 11.1 wordt, onder vervanging van de punt aan het slot van onderdeel j door een puntkomma, een onderdeel ingevoegd, luidende:
k. College bescherming persoonsgegevens: het College bescherming persoonsgegevens, bedoeld in de Wet bescherming persoonsgegevens.

B

In artikel 11.3a, eerste, derde, vierde en vijfde lid, wordt "de Autoriteit Consument en Markt" telkens vervangen door: het College bescherming persoonsgegevens.

C

Artikel 15.1 wordt als volgt gewijzigd:

1. Onder vernummering van het tweede en derde lid tot derde en vierde lid wordt een nieuw tweede lid ingevoegd, luidende:

2. Met het toezicht op de naleving van het bepaalde bij of krachtens artikel 11.3a zijn belast de bij besluit van het College bescherming persoonsgegevens aangewezen ambtenaren.

2. In de eerste volzin van het derde lid wordt "eerste lid" vervangen door: eerste en tweede lid.

3. In het vierde lid wordt "eerste lid" vervangen door: eerste en tweede lid.

D

Artikel 15.2 wordt als volgt gewijzigd:

1. In het tweede lid wordt "artikel 15.1, tweede lid" vervangen door: artikel 15.1, derde lid.

2. Onder vernummering van het derde en vierde tot vierde en vijfde lid wordt na het tweede lid een lid ingevoegd, luidende:

3. Het College bescherming persoonsgegevens is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de verplichtingen, gesteld bij of krachtens de in artikel 15.1, tweede lid, bedoelde bepalingen.

E

Aan artikel 15.4 wordt een lid toegevoegd, luidende:

4. Het College bescherming persoonsgegevens kan een bestuurlijke boete opleggen van ten hoogste € 450.000 ter zake van overtreding van de bij of krachtens de in artikel 15.1, derde lid, bedoelde regels, alsmede van artikel 5:20 van de Algemene wet bestuursrecht.

F

Artikel 15.5 wordt als volgt gewijzigd:

1. In het eerste lid wordt "artikel 15.1, eerste, tweede, onderscheidenlijk derde lid" vervangen door: artikel 15.1, eerste, tweede, derde, onderscheidenlijk vierde lid.

2. In het tweede lid wordt "artikel 15.1, eerste lid, onderscheidenlijk derde lid" vervangen door: artikel 15.1, eerste en tweede lid, onderscheidenlijk vierde lid

G

In het eerste en tweede lid van artikel 15.7 wordt "artikel 15.1, eerste lid" vervangen door: artikel 15.1, eerste en tweede lid.

**Artikel III**

In de artikelen 7 en 11 van bijlage 2 bij de Algemene wet bestuursrecht komt onderdeel b van de zinsnede met betrekking tot de Telecommunicatiewet te luiden:
b. de artikelen 3.10, 15.2, derde lid, 15.4, vierde lid en 18.9, eerste en tweede lid

**Toelichting**

Zoals in de nota naar aanleiding van het verslag is aangekondigd, strekken de onderstaande wijzigingen ertoe, de meldplicht datalekken te verduidelijken en te vereenvoudigen en daarmee voor de praktijk beter hanteerbaar te maken. Deze nota van wijziging wordt ingediend, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken.

Over de nota van wijziging is overleg gevoerd met vertegenwoordigers van de betrokken ministeries, het College bescherming persoonsgegevens (hierna: Cbp), de Autoriteit Consument en Markt en VNO-NCW-MKB Nederland. Van het Cbp is op 20 februari jl. een schriftelijke reactie ontvangen. Het Cbp vreest dat de reikwijdte van de meldplicht te zeer wordt ingeperkt waardoor deze niet wezenlijk bijdraagt aan de bescherming van persoonsgegevens in het algemeen en versterking van de positie van de burger in het

bijzonder. Naar aanleiding van de reactie van het Cbp is de toelichting op de wijzigingen van artikel 34a, eerste en zesde lid, genuanceerd. Vooropgesteld zij dat het niet de bedoeling is om een hoge drempel op te werpen voor het doen van een melding aan de toezichthouder; beoogd is te verduidelijken dat alleen datalekken met "ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens" aan het Cbp dienen te worden gemeld. Verder is verduidelijkt dat de meldingsverplichtingen niet gelden indien de gelekte gegevens op passende wijze zijn beschermd omdat dan geen nadelige gevolgen voor de privacy zijn te duchten.
De wijzigingen beogen een beter evenwicht tussen enerzijds de belangen die zijn gediend met een goede bescherming van persoonsgegevens en anderzijds de administratieve lasten en nalevingskosten die met de introductie van wettelijke meldingsverplichtingen gepaard gaan.

De kern van de wijziging betreft een herformulering van het eerste en zesde lid van artikel 34a. Met de gewijzigde formulering van het eerste lid komt beter tot uitdrukking dat de regering, gelet op de ruime werkingssfeer van de Wet bescherming persoonsgegevens (hierna: Wbp), een geclausuleerde meldplicht beoogt. Niet "alle" inbreuken op de beveiliging van persoonsgegevens behoeven bij de toezichthouder (Cbp) te worden gemeld, maar alleen die inbreuken die "ernstige" nadelige gevolgen hebben voor de bescherming van de verwerkte persoonsgegevens (eerste lid).
Een inbreuk met ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, moet daarnaast ook aan de betrokkene worden gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (tweede lid). Met het oog hierop, zal van de verantwoordelijke, op grond van het vierde lid, worden verlangd dat hij bij de melding aan het Cbp aangeeft of hij voornemens is om ook de betrokkene van de inbreuk in kennis te stellen. Het Cbp kan de melding aan de betrokkene zo nodig afdwingen (zevende lid).

In het zesde lid is verduidelijkt dat indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de getroffen persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van die gegevens, de meldingsverplichtingen van artikel 34a, eerste en tweede lid, niet van toepassing zijn. In die gevallen gaat het dwingend voorschrijven van meldingsverplichtingen, bezien vanuit de centrale doelstelling van dit wetsvoorstel -het versterken van de naleving van de algemene verplichting om persoonsgegevens op een goede en zorgvuldige manier tegen verlies of onrechtmatige verwerking te beveiligen (artikel 13 Wbp)- te ver.
Een en ander laat uiteraard onverlet dat het de verantwoordelijke vrij staat, om ook bij geringere incidenten die niet onder de meldingsplicht vallen, de getroffen personen te informeren over het incident en over de maatregelen die de verantwoordelijke heeft getroffen om de gevolgen te beperken en herhaling te voorkomen. Denk bijvoorbeeld aan een hack van de ledenadministratie van een sportvereniging. Het lijkt niet meer dan vanzelfsprekend dat het bestuur van de vereniging de leden daarover informeert. Het gaat echter te ver om een situatie als deze onder een wettelijke meldingsverplichting te brengen.
De verduidelijking van de meldplicht is eveneens van belang omdat het niet of niet volledig naleven ervan door het Cbp met een bestuurlijke boete kan worden bestraft. De formulering van een voorschrift dat door punitieve sancties wordt gehandhaafd luistert nauw in verband met het lex certa-beginsel (artikel 16 Grondwet, artikel 15 IVBPR, en artikel 7 EVRM, artikel 5:4 Awb).
De wijzigingen worden achtereenvolgens toegelicht.

A
Dit betreft een aanpassing van artikel 14 (relatie verantwoordelijke - bewerker) in verband met de herformulering van de meldplicht van artikel 34a, eerste lid.

B2

Dit betreft herstel van een omissie. Het opschrift van hoofdstuk 5 luidt "Informatieverstrekking aan de betrokkene". Voorgesteld wordt om daaraan toe te voegen: en de meldplicht bij inbreuken op de beveiliging van persoonsgegevens aan het College.

B3
Dit betreft enkele wijzigingen van artikel 34a. De meldplicht aan het Cbp (eerste lid) is geherformuleerd. Er is nauwer aangesloten bij de formulering van de meldplicht van artikel 11.3a, eerste lid, van de Telecommunicatiewet. Net als bij die meldplicht het geval is, moeten de nadelige gevolgen voor de bescherming van de persoonsgegevens zich hebben voorgedaan. Dat wil zeggen dat de gegevens daadwerkelijk zijn blootgesteld aan verlies of onrechtmatige verwerking. In de huidige formulering van de artikel 34a, eerste lid, is voldoende dat "redelijkerwijs" kan worden aangenomen dat een "aanmerkelijke kans" op nadelige gevolgen bestaat. Daarmee lijkt de meldplicht ruimer te zijn dan in de Telecommunicatiewet, terwijl dat niet is beoogd.
Zoals hiervoor reeds is opgemerkt heeft de regering van meet af aan een clausulering van de meldplicht beoogd, gelet op de ruime werkingssfeer van de Wbp. De clausulering is in het eerste lid tot uitdrukking gebracht door te spreken over "een inbreuk op de beveiliging, bedoeld in artikel 13, die *ernstige* nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens." Bij de beoordeling of er sprake is van ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens zijn vooral aard en omvang van de inbreuk van belang, de aard van de gelekte persoonsgegevens en de mate waarin technische beschermingsmaatregelen zijn getroffen ten aanzien van de desbetreffende persoonsgegevens.
Ter illustratie kan worden opgemerkt dat een beveiligingsincident (hack) inzake een ict-systeem waarin gevoelige persoonsgegevens van burgers zijn opgeslagen eerder een meldingsplichtige inbreuk bij het Cbp oplevert, dan bijvoorbeeld een incident in verband met bescherming van persoonsgegevens bij een gemeentelijke website waarop kan worden ingeschreven op een gratis jeugdsportpas.

Door de meldplicht aan het Cbp te clausuleren worden inbreuken met geringe nadelige gevolgen voor de bescherming van persoonsgegevens van de meldplicht uitgezonderd. Anders dan het Cbp in zijn brief van 20 februari 2014 aangeeft, gaat het bij de meldplicht aan het Cbp om een inschatting van de ernst van de nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens en niet om daadwerkelijk gebleken ernstig misbruik van persoonsgegevens. Een en ander vergt een beoordeling door de verantwoordelijke in het licht van de feiten en omstandigheden van het concrete geval, rekening houdend met de hierboven genoemde aspecten.

Het zesde lid wordt eveneens geherformuleerd. Het huidige zesde lid bepaalt dat de melding aan de betrokkene achterwege kan blijven 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. De reden is dat in dat geval ongunstige gevolgen voor de persoonlijke levenssfeer van de getroffen persoon niet waarschijnlijk zijn. Het is bij nadere beschouwing niet logisch dat de uitzondering alleen wordt gemaakt voor de melding aan de betrokkene en niet voor de melding aan het Cbp. Indien persoonsgegevens op passende wijze zijn versleuteld, zullen immers ook geen (ernstige) nadelige gevolgen voor de bescherming van deze gegevens te duchten zijn. In verband hiermee wordt in het zesde lid bepaald dat de meldingsverplichtingen van het eerste en tweede lid niet gelden indien passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens. Deze formulering dekt niet alleen versleuteling maar ook technieken die persoonsgegevens ontoegankelijk kunnen maken als zich een datalek voordoet (bijv. een remote wipe bij een verloren of gestolen smartphone).

De verantwoordelijkheid voor de beoordeling of aan het criterium van het zesde lid is voldaan ligt bij de verantwoordelijke. Zou de verantwoordelijke daarmee lichtvaardig omgaan en aannemen dat een versleuteling passend is, terwijl de versleutelingsmethode achterhaald is en om die reden geen bescherming biedt tegen kennisname door personen die daartoe niet gerechtigd zijn, dan loopt de verantwoordelijke het risico daarvoor door het Cbp een bestuurlijke boete opgelegd te krijgen.
De verantwoordelijke doet er bij twijfel over de kwaliteit van de technische beschermingsmaatregelen dan ook verstandig aan om wel een melding te doen bij het Cbp als gelet op de feiten en omstandigheden van het geval ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens niet uit te sluiten zijn. Het Cbp wordt op deze wijze in staat gesteld om de kwaliteit van de technische beschermingsmaatregelen te beoordelen. Dit is met name van belang omdat het Cbp zo nodig een melding aan betrokkene kan afdwingen indien waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer te duchten zijn. Het oordeel van het Cbp is hierbij doorslaggevend (zevende lid).

Het Cbp bevindt zich hiermee in een wat andere positie dan de Autoriteit Consument en Markt (hierna: ACM) op grond van de Telecommunicatiewet (art. 11.3a, vijfde lid, Tw). De aanbieder van een openbare elektronische communicatiedienst moet ACM moet in het kader van het mogelijk achterwege laten van een kennisgeving aan de betrokkene om een voorafgaand oordeel vragen over de technische beschermingsmaatregelen die zijn getroffen. Indien ACM van oordeel is dat de technische beschermingsmaatregelen passend zijn, mag de aanbieder van de openbare elektronische communicatiedienst kennisgeving aan de betrokkene achterwege laten.
In het wetsvoorstel zoals dat bij de Tweede Kamer is ingediend is de voorafgaande beoordeling van de kwaliteit van de technische beschermingsmaatregelen door het Cbp reeds losgelaten.

Voorgesteld wordt om het achtste lid te schrappen. Het opleggen van een zelfstandige (met een bestuurlijke boete te sanctioneren) verplichting om intern binnen de organisatie een overzicht bij te houden van alle inbreuken (de ernstige en de minder ernstige), is bij nader inzien minder wenselijk gelet op de lasten die een dergelijke verplichting met zich brengt. Uit de algemene beveiligingsverplichting van artikel 13 Wbp vloeit reeds voort dat de verantwoordelijke procedures heeft voor het tijdig en doeltreffend behandelen van beveiligingsincidenten en afgehandelde incidenten gebruikt om de beveiliging waar mogelijk structureel te verbeteren.
Handhaving van de meldplicht van artikel 34a door het Cbp kan op de gebruikelijke wijze lopen, via signalen van gedupeerde burgers, belangenorganisaties, of berichten in de media. De registratieplicht van het achtste lid is daarvoor niet nodig.

De wijzigingen van het vierde en het zevende lid zijn louter technisch. De wijziging van het vierde lid sluit aan op de gewijzigde bewoordingen van het eerste lid. Het zevende lid is in overeenstemming gebracht met het tweede lid.

C
De wijziging onder 1 betreft een technische correctie op artikel 51a, eerste lid, dat de samenwerking tussen het Cbp en andere toezichthouders regelt. Bij nadere beschouwing is de vormgeving van de samenwerking niet geheel evenwichtig. Om die reden zijn de leden 2 en 3 ineen geschoven. Het nieuwe tweede lid bepaalt dat het College en de andere toezichthouders bevoegd zijn om uit eigen beweging en desgevraagd verplicht aan elkaar de gegevens betreffende de verwerking van persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van hun taak.
Het vierde lid lijkt bij nader inzien een overbodige norm; persoonsgegevens mogen uitsluitend worden gedeeld voor zover dat noodzakelijk is voor de uitoefening van de taak van de verstrekkende of ontvangende toezichthouder. Het is om die reden niet nodig om te bepalen dat verstrekking niet plaatsvindt indien de persoonlijke levenssfeer

van de betrokkene daardoor onevenredig wordt geschaad. Dit ligt reeds besloten in het noodzaak-criterium.

D
Dit betreft een beperkte aanvulling van artikel 43a Wbp. Er kunnen situaties zijn waarin de in artikel 43, onder e, benoemde belangen (met name "de rechten en vrijheden van anderen") vergen dat de verplichting van artikel 34a, tweede lid, die dwingende mededeling aan betrokkene voorschrijft indien een inbreuk waarschijnlijk ongunstige gevolgen heeft voor de bescherming van de persoonlijke levenssfeer, buiten toepassing blijft. Voor de instellingen in de financiële sector is hierin voorzien in artikel 34a, lid 9. In aansluiting hierop lijkt het raadzaam om in artikel 43 een algemene uitzonderingsmogelijkheid te creëren. Ook andere situaties zijn immers voorstelbaar, waarin het van belang is dat mededelingen aan het publiek achterwege blijven. Denk bijv. aan het proces rondom de overname van een beursgenoteerde onderneming. Mocht zich daarbij onverhoopt een inbreuk voordoen met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, dan kan mogelijk worden volstaan met melding aan het Cbp. Zo nodig kan het Cbp de bevoegdheid van artikel 34a, zevende lid, aanwenden als het van oordeel is dat de verantwoordelijke wel een kennisgeving aan de betrokkene zou dienen te doen.

E
Dit nieuwe artikel voegt een samenloopbepaling toe. De Telecommunicatiewet wordt gewijzigd in een bij de Eerste Kamer aanhangig wetsvoorstel, dat vermoedelijk eerder in werking treedt dan het onderhavige wetsvoorstel. De wijzigingen zijn wetstechnisch van aard.

De Staatssecretaris van Veiligheid en Justitie,