Privacy & Data Protection Update

NautaDutilh

Bill on notification of data leaks / Wetsvoorstel meldplicht datalekken **28 June 2013**

This newsletter is sent by NautaDutilh

Bill on notification of data leaks

*This bill introduces a duty to notify the Dutch Data Protection Authority (College Bescherming Persoonsgegevens, the "**CBP**") and the relevant data subject(s) in the event of a breach of security measures for the protection of personal data. The duty will apply to businesses, governmental bodies and others, provided in all cases that they constitute a "data controller" within the meaning of the Personal Data Protection Act (Wet bescherming persoonsgegevens, the "**PDPA**"). The rule imposing the duty will be set out in a new provision of the PDPA (Article 34a).*

The penalty for non-compliance with this duty will be a fine of up to EUR 450,000. A similar fine can be imposed for failure to co-operate in an investigation by the CBP into a breach/possible breach (of the above duty to notify) pursuant to article 5:20 of the General Administrative Law Act (Algemene wet bestuursrecht). This article lays down a general duty to co-operate and therefore such a fine can also be imposed in cases where the CBP is conducting an investigation other than in connection with article 34a of the PDPA.

To whom must a notification be made?

1. The CBP must *immediately* be notified of a *breach of security measures* if it can *reasonably* be assumed that, as a result of the breach, there is a *significant risk* of *negative consequences for the protection of personal data* being processed.

2. The data subject must *immediately* be notified of *a breach as described above* if the breach will *probably have unfavourable consequences* for his/her individual privacy.

The explanatory memorandum to the bill states that the assessment of a breach must be carried out as objectively as possible, based on the actual facts and circumstances of the case in question. Whether the loss of a mobile telephone or USB stick or the theft of a laptop, for example, must be notified will depend on the type of data and the likely risk for the data subject and the enterprise.

An example given in the explanatory memorandum is that if the membership records of a sport association are lost or hacked, this will usually cause inconvenience to the association and its members but is unlikely to necessitate a notification to the CBP. The consequences of a data leak of this type will usually be of a limited nature; in addition, the data subjects can be expected to have accepted a certain degree of risk. A data leak at the tax authorities, a bank or an insurer, however, is usually of a different order. Such a leak can lead to financial loss on the part of the data subject(s) or can result in data that are protected by a duty of confidentiality being compromised. The CBP will probably draw up guidelines to provide more clarification.

What information must be given in the notification?

1. Both the CBP and the data subject(s) must in any event be notified of the following: i) the nature of the breach, ii) the parties from which more information about the breach can be obtained and iii) the recommended measures for limiting the negative consequences of the breach.

The explanatory memorandum states that, with regard to the nature of the breach, a general description will usually be sufficient. A data subject who wishes to know more about his/her

individual situation can contact the business. For this reason, contact information must be given in the notification. With regard to recommended measures, these could be the changing of usernames and passwords or notification of a credit card company. This is also of significance in connection with a defence, in a liability action, that the data subject himself/herself was at fault.

The information set out in the notification, as well as the actual text of the notification to the data subject(s), must be retained by the data controller itself. The latter is required to maintain a record of *all* breaches, including breaches that have been detected but not notified. Based on the protocol it must be possible to show which breaches have been detected and which measures have been taken.

According to the explanatory memorandum, it is expected that the great majority of notifications to the CBP will not give rise to the need for an investigation or enforcement measures. The CBP will examine the notifications and assess whether there is reason to initiate an investigation. If such an investigation is initiated, this can subsequently result in enforcement measures. Factors that will play a role in the CBP's assessment include the extent of the data leak, the leak's potential consequences and the type of data in question. It cannot as yet be predicted what proportion of the notifications will give rise to the need for further action.

2. The notification to the CBP must, in addition, contain a description of i) the detected consequences and the probable consequences of the breach for the processing of personal data and ii) the measures that the data controller has taken or proposes to take in order to remedy those consequences.

This information will mostly be of a technical nature. In some cases, the information required to be notified may include technical details of a confidential nature. According to the explanatory memorandum, the relevant business can, if it so wishes, explicitly designate such data as "company-confidential" (*bedrijfsvertrouwelijk*) within the meaning of article 10(1)(c) of the Open Government Act (*Wet openbaarheid van bestuur*).

Manner of notification to data subject(s)

1. The notification to the data subject(s) must be such as to ensure that the provision of information is carried out in a proper and careful manner, taking into account the nature of the breach, the detected consequences and the factual consequences of the breach for the processing of personal data, the circle of data subjects affected and the costs.

The explanatory memorandum states that in cases where the breach affects a relatively limited number of data subjects, these can be approached personally and in a tailored manner. If, however, a larger number of data subjects is affected, a newspaper advertisement in addition to a website announcement would be considered more appropriate.

Exceptions

1. Notification to the data subject(s) is not required if appropriate technological protection measures have been taken to ensure that the personal data in question are encrypted or otherwise rendered unintelligible to parties that are not entitled to access those data.

2. If no notification has been made to the data subject(s), the CBP may demand that the data subject(s) be notified if it is of the opinion that the breach is likely to have negative consequences for the individual privacy of the data subject(s).

3. The notification requirement does not apply if the data controller is a provider of public electronic communications services and, in that capacity, has made a notification as referred to in article 11.3a(1) and (2) of the Telecommunications Act (*Telecommunicatiewet*). The latter provision sets out a specific notification requirement for providers of public electronic communications services (in connection with the provision of public electronic communications services).

Currently such providers need to notify the Authority for Consumers and Markets. If the bill is adopted they will have to notify the CBP instead of the Authority for Consumers and Markets.

The described exception does not apply in situations where the data controller is a different party than the provider of the public electronic communications services (for example, where the provider is a data processor within the meaning of the PDPA). In such a case, each of the two parties will be subject to a notification duty (under article 34a of the PDPA and under article11.3a

of the Telecommunications Act, respectively). If the provider is itself the data controller, its notification duty will be pursuant to article 11.3a of the Telecommunications Act.

4. Financial institutions within the meaning of the Financial Supervision Act (*Wet op het financieel toezicht*, the "**FSA**") will not be required to notify a breach to the relevant data subject(s), but will still have to notify it to the CBP.

Such institutions are subject to a notification duty under the FSA, as well as the Prudential Rules (Financial Supervision Act) Decree and the Financial Institutions Business Conduct Supervision Decree. According to the explanatory memorandum, in the financial sector it would be too risky (partly in view of the financial crisis) to make public notifications to data subjects mandatory. A financial institution's duty of care provides a sufficient guarantee that the institution will carry out its responsibility towards its clients by contacting them directly.

A financial institution will only be subject to a double notification requirement (to both the CBP and the Dutch Central Bank/Authority for the Financial Markets) if a data leak also constitutes an *incident* within the meaning of the FSA (and the Decrees mentioned above). Such an *incident* is conduct or an event that poses a serious threat to the sound conduct of the financial institution's business.

Data processors

If your enterprise (as a data controller of personal data) engages one or more parties (data processors) to process such personal data on the instruction of, and on behalf of, the data controller, it is important that the notification duty is taken into account in the (data processor) agreement(s). The data processor must, at a minimum, be required to notify the data controller of any breach of security where it can reasonably be assumed that, as a result of the relevant breach, there is a significant risk of negative consequences for the personal data processed by that data processor.

As the wording of the above rule could give rise to many questions, it is probably preferable to make the notification requirement in the agreement more comprehensive and to include additional safeguards. The CBP has set out a checklist in this regard in its guidelines on the protection of personal data (see our earlier newsletter on this subject).

Expected future developments

Further rules on notifications (their content and the manner in which they must be made) may be laid down in one or more general administrative orders. In addition, it has been announced that amendments to the bill will be submitted, consisting of rules aimed at strengthening the enforcement of the PDPA by broadening the powers of the CBP (e.g. to impose fines).

Finally, there are plans to introduce statutory notification requirements for, e.g., i) providers of certification services and ii) certain sectors in which cyber incidents could potentially have a disruptive impact on society.

To be continued.

Click here for the text of the bill (in Dutch)

Click here for the text of the explanatory memorandum to the bill (in Dutch)

Wetsvoorstel meldplicht datalekken

*In dit wetsvoorstel wordt een meldplicht geïntroduceerd om een inbreuk op beveiligingsmaatregelen te melden bij het College Bescherming Persoonsgegevens ("**CBP**") en aan betrokkene(n). De meldplicht zal gelden voor bedrijven, de overheid, e.a. mits zij als "verantwoordelijke" in de zin van de Wet bescherming persoonsgegevens ("**Wbp**") zijn aan te merken. De meldplicht wordt opgenomen in (een artikel 34a van) de Wbp.*

Het niet voldoen aan de meldplicht kan leiden tot een boete van maximaal EUR 450.000. Ook het niet naleven van de medewerkingsplicht in het kader van een onderzoek door het CBP ingevolge artikel 5:20 van de Algemene wet bestuursrecht kan leiden tot een dergelijke boete. Dit betreft dan ook het niet naleven van de medewerkingsplicht in gevallen van onderzoek naar andere overtredingen dan artikel 34a Wbp.

Bij wie moet worden gemeld?

1. Het CBP moet *onverwijld* in kennis worden gesteld van een *inbreuk op de beveiligingsmaatregelen*, waarvan *redelijkerwijs* kan worden aangenomen dat die leidt tot een *aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens* die worden verwerkt.

2. De betrokkene dient *onverwijld* in kennis te worden gesteld van een *dergelijke inbreuk*, indien deze inbreuk *waarschijnlijk ongunstige gevolgen zal hebben* voor diens persoonlijke levenssfeer.

De Memorie van Toelichting ("**MvT**") vermeldt dat de beoordeling van een inbreuk zo geobjectiveerd mogelijk moet zijn. Er moet worden gekeken naar de feitelijke omstandigheden van het geval. Of het verlies van bijvoorbeeld een mobiele telefoon, de diefstal van een laptop of het zoekraken van een USB stick moet worden gemeld, is ook afhankelijk van de aard van de data en het vermoedelijke risico dat de betrokkene en de onderneming lopen.

De MvT vermeldt als voorbeeld dat het zoekraken of hacken van de ledenadministratie van een sportvereniging doorgaans zal leiden tot het nodige ongemak voor de vereniging en leden, maar niet snel aanleiding zal hoeven te geven tot een melding bij het CBP. De gevolgen van een dergelijk datalek blijven doorgaans beperkt en ook van betrokkenen kan worden gevergd dat zij een zekere mate van risico aanvaarden. Maar een datalek bij de Belastingdienst, of een bank of verzekeraar is doorgaans van een andere orde. Een dergelijk datalek kan leiden tot financieel nadeel bij de betrokkene(n) of tot compromittering van gegevens die worden beschermd door een geheimhoudingsplicht. Het CBP zal waarschijnlijk richtlijnen opstellen om de praktijk enige houvast te geven.

Wat moet worden gemeld?

1. Zowel aan het CBP als aan de betrokkene(n) omvat de kennisgeving in ieder geval: i) de aard van de inbreuk, ii) de instanties waar meer informatie over de inbreuk kan worden verkregen en iii) de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

De MvT vermeldt dat bij de aard van de inbreuk doorgaans met een algemene omschrijving zal kunnen worden volstaan. Als de betrokkene wil weten waar hij persoonlijk aan toe is, kan hij contact opnemen met het bedrijf. Daarom moeten contactgegevens worden vermeld in de kennisgeving. Wat betreft de aanbevolen maatregelen kan worden gedacht aan het veranderen van gebruikersnamen en wachtwoorden, of het melden bij de creditcardmaatschappij. Dit is ook van belang voor aansprakelijkheidsclaims in verband met een beroep op "eigen schuld van de betrokkene".

Overigens dient deze in de kennisgeving opgenomen informatie, alsmede de tekst van de kennisgeving aan betrokkene(n) ook te worden bewaard door de verantwoordelijke zelf. Deze dient een overzicht bij te houden van *alle* inbreuken. Dit betreft dus ook inbreuken die wel zijn geconstateerd, maar niet zijn gemeld. Aan de hand van het protocol zou overigens moeten kunnen worden aangetoond welke inbreuk is geconstateerd en welke maatregelen zijn genomen.

De MvT vermeldt dat verwacht wordt dat het overgrote deel van meldingen bij het CBP geen aanleiding zal geven tot een onderzoek of handhavingsmaatregelen. Het CBP zal de meldingen beoordelen en een inschatting moeten maken of er aanleiding is een onderzoek in te stellen. Een dergelijk onderzoek kan vervolgens leiden tot handhavingsmaatregelen. Factoren als de omvang van het datalek, de potentiële gevolgen ervan en de aard van de gegevens zullen een rol spelen bij deze afweging door het CBP. Het valt nog niet te voorzien in hoeveel gevallen de meldingen aanleiding zullen geven tot verdere actie.

2. De kennisgeving aan het CBP omvat daarnaast een beschrijving van i) de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en ii) de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

Deze informatie zal veelal technisch van aard zijn. Het kan zijn dat melding moet worden gemaakt van technische details die van vertrouwelijke aard zijn. Bedrijven kunnen dergelijke gegevens volgens de MvT desgewenst expliciet als bedrijfsvertrouwelijk aanmerken in de zin van artikel 10, eerste lid onder c, van de Wet openbaarheid van bestuur.

Hoe melden aan betrokkene(n)?

1. De kennisgeving aan de betrokkene(n) moet op zodanige wijze worden gedaan 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.

De MvT vermeldt dat wanneer de inbreuk zich beperkt tot een verhoudingsgewijs klein aantal betrokkenen, deze persoonlijk en gericht kunnen worden benaderd. Als de inbreuk een groot aantal betrokkenen betreft zou naast een bekendmaking op een website een advertentie in de dagbladen meer in de rede liggen.

Uitzonderingen

1. De kennisgeving aan de betrokkene(n) is niet vereist indien gepaste technische beschermingsmaatregelen zijn 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.

2. Indien geen kennisgeving is gedaan aan de betrokkene(n), kan het CBP, indien het van oordeel is dat de inbreuk waarschijnlijk nadelige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene(n), verlangen dat alsnog een kennisgeving wordt gedaan.

3. Het meldplicht artikel is niet van toepassing indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet ("Tw"). Dit artikel bevat een specifieke meldplicht voor aanbieders van openbare elektronische communicatiediensten (in verband met de levering van openbare elektronische communicatiediensten).

Dergelijke aanbieders moeten overigens nu melden bij de Autoriteit Consument en Markt. Ingevolge het wetsvoorstel zullen zij in plaats daarvan moeten gaan melden bij het CBP.

Deze uitzondering geldt niet in situaties waarin de verantwoordelijke een ander is dan de aanbieder van de openbare elektronische communicatiedienst (bijvoorbeeld in het geval de aanbieder een bewerker is in de zin van de Wbp). In dat geval zouden beide partijen een melding moeten doen (op grond van artikel 34a Wbp, respectievelijk 11.3a Tw). Indien de verantwoordelijke dezelfde is als de aanbieder van de openbare elektronische communicatiedienst doet deze de melding op grond van artikel 11.3a Tw.

4. Financiële ondernemingen als bedoeld in de Wet op het financieel toezicht ("**Wft**") hoeven betrokkene(n) niet op de hoogte te stellen, maar moeten wel melden bij het CBP.

Financiële ondernemingen hebben een meldplicht ingevolge de Wft (en het Besluit prudentiële regels Wft en het Besluit gedragstoezicht financiële ondernemingen). Openbare kennisgevingen aan betrokkenen worden in de financiële sector - mede tegen de achtergrond van de financiële crisis - als te risicovol ervaren om dwingend te worden voorgeschreven. De zorgplicht van de financiële onderneming zal waarborgen dat zij haar verantwoordelijkheid jegens haar cliënten in rechtstreeks contact met die cliënten zal nemen.

Een dubbele meldplicht bij het CBP respectievelijk de DNB of AFM bestaat alleen als een datalek eveneens een *incident* is in de zin van de Wft (en bovengenoemde Besluiten). Een dergelijk *incident* is een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de financiële onderneming.

Bewerkers

Voor zover uw onderneming (als verantwoordelijke voor persoonsgegevens) bewerkers inschakelt die deze persoonsgegevens in opdracht van en ten behoeve van de verantwoordelijke verwerken, is het belangrijk in de (bewerkers)overeenkomst rekening te houden met deze meldplicht. De bewerker zou minimaal verplicht moeten zijn tot melding aan de verantwoordelijke van een inbreuk op de beveiliging waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt.

Gelet op deze open norm is het waarschijnlijk wenselijk de meldplicht in de overeenkomst wat ruimer te formuleren en aanvullende waarborgen op te nemen. Het CBP heeft hiervoor een checklist opgenomen in de Richtsnoeren beveiliging van persoonsgegevens (zie onze eerdere nieuwsbrief over dit onderwerp).

Toekomstige ontwikkelingen

Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de (inhoud en wijze van) kennisgeving. Daarnaast is aangekondigd dat nog een nota van wijziging op het onderhavige wetsvoorstel zal worden ingediend die voorziet in een regeling die strekt tot uitbreiding van de bestuurlijke (boete)bevoegdheden van het CBP met het oog op de versterking van de handhaving van de Wbp.

Tenslotte zullen nog andere wettelijke meldplichten volgen voor bijvoorbeeld i) certificatiedienstverleners ten aanzien van gekwalificeerde certificaten en ii) bepaalde sectoren waar cyberincidenten een potentieel maatschappelijk ontwrichtende werking kunnen hebben.

Wordt vervolgd.

Klik hier voor het (Nederlandstalige) Wetsvoorstel

Klik hier voor de (Nederlandstalige) Memorie van Toelichting

Contact

For the Netherlands / voor Nederland:
Jacqueline van Essen
T: +31 20 7171 714

For Belgium / voor België:
Julien Hick
T: +32 2 566 8518

For Luxembourg / voor Luxemburg:
Vincent Wellens
T +35 2 261 22934