Privacy e-Newsletter

NautaDutilh

Public consultation on proposed changes to Personal Data Protection Act/Consultatie wijziging Wet bescherming persoonsgegevens **20 January 2012**

This newsletter is sent by NautaDutilh

Public consultation on proposed changes to Personal Data Protection Act

The Ministry of Security and Justice is currently conducting a public consultation on a draft bill to amend the Dutch Personal Data Protection Act.

The draft bill aims to extend the scope for using images from individuals' and businesses' surveillance cameras for the investigation of criminal offences. It also proposes the introduction of a notification requirement regarding data leaks.

Individuals and businesses can participate in the consultation at http://www.internetconsultatie.nl/camerabeelden

The consultation period for the draft bill to amend the Personal Data Protection Act will run until 29 February 2012. The two most important changes are described below.

1. Use of surveillance camera images for investigating criminal offences

Under the proposed new rules, camera images of criminal offences recorded by businesses or private individuals may be published (e.g. on the internet or on screens in shopping centres) if there has either been a prior investigation by the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*) or if suitable and specific guarantees are in place. These guarantees are to be elaborated on in a general administrative order, and will be based on those applicable under the rules on communications to the public in connection with criminal investigations (as laid down in the *Aanwijzing Opsporingsberichtgeving*).

2. Notification requirement regarding data leaks

Businesses and government bodies will be required to report breaches of security measures for the protection of personal data if they become aware of such a breach. The incident must be notified to the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*, "CBP") and to the relevant data subject(s) if there is a significant risk that the leaked data have been or will be lost or unlawfully processed. Administrative fines may be imposed in the event of non-compliance.

More specifically, the rules stipulate:

- The CBP must immediately be notified of a breach of security measures if it can reasonably be assumed that, as a result of that breach, there is a significant risk that the leaked data have been or will be lost or unlawfully processed, adversely affecting the personal data and privacy of the data subject(s).

  The explanatory memorandum to the draft bill states that it must be determined as objectively as possible, based on an assessment of the facts and circumstances of the case at hand, that a significant risk as described above reasonably exists. The memorandum also states that it is expected that the CBP will draw up policy rules on fines and that these will indirectly provide a degree of practical guidance.

Following receipt of the notification, the CBP will assess whether it is necessary to conduct an investigation or to issue instructions. It may also choose not to respond to the notification.

- The relevant data subject(s) must also immediately be notified of the breach.
- The CBP as well as the data subject(s) must in any event be notified of the nature of the breach, the bodies or organisations from which more information about the breach can be obtained and the recommended measures for limiting the negative consequences of the breach.
- The notification to the CBP must also include a description of the identified and the probable consequences of the breach on the processing of personal data, in addition to the measures the responsible party has taken or proposes to take in order to remedy these consequences.
- 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 identified and the actual consequences of the breach on the processing of personal data, the circle of data subjects affected and the costs.

  The explanatory memorandum states, for example, 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.

- Notification to the data subject(s) is not required if, in the CBP's opinion, the responsible party has taken appropriate technological protection measures to ensure that the personal data in question are encrypted or otherwise rendered unintelligible to parties that are not entitled to access those data.
- If the responsible party does not notify the data subject(s) of the breach, the CBP may – if it decides that the breach is likely to adversely affect the personal data and privacy of the data subject(s) – demand that the latter be notified.
- Records must be kept of all breaches.
- Further rules on the notification may be laid down in general administrative orders.
- The CBP may impose a maximum fine of EUR 200,000 in the event of failure to comply with the abovementioned obligations.

The above also affects contracts with data processors (i.e. external parties that process personal data for and on behalf of the responsible party).

<u>The notification requirement pursuant to the Personal Data Protection Act will not apply</u>:

- if the responsible party is a provider of electronic communications services and, in that capacity, has made a notification as referred to in Article 11.3a(1) and (2) of the Dutch Telecommunications Act. Under the new rules, such notifications will have to be made to the CBP instead of OPTA (the Independent Post and Telecommunications Authority);
- if the responsible party has an obligation, pursuant to Article 3:10(3) or Article 4:11(4) of the Financial Supervision Act, to provide information to the Dutch Central Bank or the Netherlands Authority for the Financial Markets. These provisions require financial institutions to inform the relevant body about incidents relating to the soundness of their business operations (*integere bedrijfsvoering*).

The explanatory memorandum explains that financial institutions are required to keep internal records of such incidents (pursuant to Article 12 of the Prudential Rules (Financial Supervision Act) Decree and Article 19 of the Financial Institutions Business Conduct Supervision Decree). Furthermore, in the event of an incident having consequences for one or more clients, the financial institution must inform the relevant client(s) about that incident. According to the explanatory memorandum, these rules sufficiently safeguard the interests of data subjects with regard to the protection of their personal data. This is because the principles of the Financial Supervision Act in this regard are largely in line with those of the draft bill: they too are directed at the preservation and, where necessary, the restoration of data subjects' trust in the responsible parties. Consequently, there is no reason to impose a double notification requirement on the financial sector, which is why the draft bill contains an exception for financial institutions that are already subject to a notification requirement pursuant to the Financial Supervision Act.

According to the explanatory memorandum there is, however, a material difference between the notification requirements pursuant to the draft bill and those pursuant to the Financial Supervision Act. The duty of confidentiality under Articles 1:89 and 1:90 of the Financial Supervision Act does not allow for notifications to data subjects regarding data leaks to be made in the manner set out under the draft bill, because the latter provides for public notifications. In the financial sector, it would be too risky (partly in view of the financial crisis) to make public notifications of this type mandatory, as it cannot be predicted whether such a notification might not lead to rumours that are incapable of being objectively dispelled, causing an unnecessary decrease of trust on the part of the public or the relevant market. However, since practice has shown that financial institutions carry out their responsibility towards their clients by contacting them directly, this ensures that the difference between the two notification requirements will not have adverse consequences for the relevant data subject(s).

For more information on this topic or on privacy, please contact (for the Netherlands) Jacqueline van Essen (T: +31 20 7171 714), Amsterdam.

Consultatie wijziging Wet bescherming persoonsgegevens

Het Ministerie van Veiligheid en Justitie heeft een voorontwerp gepubliceerd van een wetsvoorstel voor aanpassing van de Wet bescherming persoonsgegevens.

Het wetsvoorstel bevat een regeling 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. In het wetsvoorstel is ook een regeling opgenomen voor een meldplicht voor datalekken.

Op http://www.internetconsultatie.nl/camerabeelden kunnen burgers en het bedrijfsleven reageren op het wetsvoorstel.

Het wetsvoorstel tot wijziging Wet bescherming persoonsgegevens ligt tot 29 februari 2012 ter consultatie. De belangrijkste twee wijzigingen worden hieronder kort beschreven.

1. Verruiming gebruik camerabeelden t.b.v. opsporing strafbare feiten

Camerabeelden van strafbare feiten gemaakt door particulieren of bedrijven mogen openbaar worden gemaakt (bijvoorbeeld op internet, of op beeldschermen in winkelcentra) wanneer er ofwel een voorafgaand onderzoek door het College Bescherming Persoonsgegevens heeft plaatsgevonden, ofwel passende en specifieke waarborgen zijn. Die waarborgen zullen nader worden uitgewerkt in een Algemene Maatregel van Bestuur waarbij zal worden aangehaakt bij de waarborgen uit de Aanwijzing Opsporingsberichtgeving.

2. Meldplicht datalekken

Bedrijven en de overheid krijgen een meldplicht in geval van gebleken doorbrekingen van getroffen maatregelen voor de beveiliging van persoonsgegevens. De melding moet worden gedaan aan het College Bescherming Persoonsgegevens ("CBP") en aan betrokkenen als aannemelijk is dat persoonsgegevens als gevolg van het lek zijn blootgesteld aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Het nalaten aan de verplichting te voldoen kan worden gesanctioneerd met een bestuurlijke boete.

De verplichting houdt meer bepaald het volgende in:

- Het CBP moet onverwijld in kennis worden gesteld van een inbreuk op beveiligingsmaatregelen waarvan redelijkerwijs kan worden aangenomen dat die 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.

  De Memorie van Toelichting vermeldt dat dit een beoordeling vergt die zo geobjectiveerd mogelijk moet zijn. Het aanmerkelijk risico moet redelijkerwijs aanwezig zijn. Dat moet naar de feitelijke omstandigheden van het geval worden vastgesteld. Tenslotte zal het CBP waarschijnlijk boetebeleidsregels vaststellen waarmee het CBP indirect enige houvast kan geven aan de praktijk.

Het CBP moet worden geïnformeerd zodat kan worden beoordeeld of een onderzoek of het geven van aanwijzingen noodzakelijk is. Een melding kan ook zonder reactie van het CBP blijven.

- De betrokkene dient ook onverwijld in kennis te worden gesteld van een dergelijke inbreuk.
- De kennisgeving aan het CBP en de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
- De kennisgeving aan het CBP 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.
- De kennisgeving aan de betrokkene wordt op zodanige wijze 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 Memorie van Toelichting vermeldt bijvoorbeeld dat wanneer de inbreuk zich beperkt tot een verhoudingsgewijs klein aantal betrokkenen, deze persoonlijk en gericht kunnen worden benaderd. Indien de inbreuk een groot aantal betrokkenen betreft, ligt naast een bekendmaking op de website een advertentie in de dagbladen meer in de rede.

- De kennisgeving aan de betrokkene is niet vereist indien de verantwoordelijke naar het oordeel van het CBP 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.
- Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het CBP, indien het van oordeel is dat inbreuk waarschijnlijk nadelige gevolgen zal hebben voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene, verlangen dat alsnog een kennisgeving wordt gedaan.
- Er dient een overzicht te worden bijgehouden van alle inbreuken.
- Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving.
- Op overtreding van bovengenoemde verplichtingen kan het CBP een boete opleggen van maximaal EUR 200.000.

Bovenstaande heeft ook gevolgen voor contracten met bewerkers; externe partijen die in opdracht van en t.b.v. de verantwoordelijke persoonsgegevens verwerken.

<u>De meldingplicht is niet van toepassing indien</u>:

- De verantwoordelijke in zijn hoedanigheid als aanbieder van een elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet. Ingevolge de nieuwe regels zal een dergelijke kennisgeving ook moeten worden gedaan bij het CBP in plaats van de OPTA.
- Op de verantwoordelijke een verplichting rust tot het verstrekken van informatie op grond van de artikelen 3:10, derde lid, of 4:11, vierde lid, van de Wet op het financieel toezicht. Deze artikelen verplichten financiële ondernemingen aan de DNB/AFM informatie te verstrekken over incidenten die betrekking hebben op een integere bedrijfsvoering.

De Memorie van Toelichting vermeldt dat financiële ondernemingen op grond van de artikelen 12 van het Besluit prudentiele regels Wft en 19 van het Besluit gedragstoezicht financiële ondernemingen Wft incidenten intern moeten vastleggen. Verder wordt vermeldt dat financiële ondernemingen hun cliënten al zo spoedig mogelijk dienen te informeren over het incident, wanneer dat gevolgen heeft of heeft gehad voor de desbetreffende cliënt. In termen van de bescherming van persoonsgegevens zijn de belangen van de betrokkene daarmee afdoende gewaarborgd, aldus de Memorie van Toelichting. Het stelsel van de Wft zou daarmee reeds in vergaande mate aan de uitgangspunten van dit wetsvoorstel voldoen. Immers, ook dit stelsel is bij uitstek gericht op het behoud, en waar nodig, herstel van vertrouwen van betrokkenen in verantwoordelijken. Er is dan ook geen aanleiding verandering aan te brengen in dit stelsel door het opleggen van dubbele meldplichten aan de financiële sector. Voorgesteld wordt dan ook om een voorziening op te nemen die inhoudt dat de meldplicht niet van toepassing is op

ondernemingen voor wie reeds een meldplicht geldt uit hoofde van de Wft.

Er is overigens volgens de toelichting wel een relevant verschil tussen de meldplichten op grond van dit wetsvoorstel en de meldplichten op grond van de Wft. De geheimhoudingsplichten van de artikelen 1:89 en 1:90 van de Wft laten geen ruimte om meldingen van datalekken door de verantwoordelijke aan de betrokkene op dezelfde wijze te doen als in het wetsvoorstel Wbp. Die regeling gaat immers uit van een openbare kennisgeving. Dergelijke openbare kennisgevingen in de financiële sector zijn - mede tegen de achtergrond van de financieel crisis - te risicovol om dwingend te worden voorgeschreven. Onvoorspelbaar is of een openbare kennisgeving kan leiden tot het ontstaan van geruchten die niet meer op zakelijke wijze ontzenuwd kunnen worden en die daardoor nodeloos aanleiding geven tot vermindering van vertrouwen van het publiek of de relevante markt. Waar de praktijk leert dat financiële ondernemingen hun verantwoordelijkheid jegens hun cliënten in rechtstreeks contact met die cliënt nemen, is verzekerd dat het verschil tussen de meldplichten geen nadelige gevolgen voor de betrokkenen heeft.

Voor meer informatie inzake dit onderwerp of privacy, kunt u voor Nederland contact opnemen met: Jacqueline van Essen (T: +31 20 7171 714), Amsterdam.

Contact

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

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

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