Privacy & Data Protection Update

NautaDutilh

New security guidelines/Nieuwe beveiligingsrichtlijnen **25 February 2013**

This newsletter is sent by NautaDutilh

New security guidelines

*On 19 February 2013, the **Dutch Data Protection Authority** (College Bescherming Persoonsgegevens, the "**CBP**") published its **new guidelines on the protection of personal data**. These guidelines will replace earlier guidelines published in 2001.*

*The guidelines will **enter into effect on 1 March 2013**. By that date, companies must have complied with a "Plan-Do-Check-Act" cycle, and their processing agreements (if any) must address the subjects specified in the guidelines.*

Pursuant to the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*) a company needs to implement appropriate technical and organisational measures to secure personal data against loss or any form of unlawful processing. The measures should guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. The measures should also aim at preventing unnecessary collection and further processing of personal data. The CBP guidelines provide further guidance on this.

The new CBP guidelines set out a "**Plan-Do-Check-Act**" cycle consisting of the following steps:
1. A risk analysis
2. Implementation of appropriate security measures based on the risk analysis
3. Periodic checks on compliance with the security measures
4. Periodic evaluation and amendments based on changed circumstances.

Many companies have their personal data processed by a **processor**: an external body that processes personal data solely for and on behalf of a company and in accordance with that company's instructions. The processor may not use the personal data for its own purposes (examples include outsourcing of the payroll processing or hosting). The new guidelines contain a list of subjects that must in any event be provided for in the **(processing) agreement** (the agreement between the company and the processor regarding the processing of personal data).

According to the CBP, the highest level of security is, as a general rule, achieved by organising information security in accordance with **generally accepted security standards** such as the Code of Practice for Information Security Management (*Code voor Informatiebeveiliging*, NEN-ISO/IEC 27002:2007.nl), to which the new guidelines frequently refer. For the development and management of web applications, for example, the National Cyber Security Centre security guidelines for web applications can be used as the point of departure.

Click here for a summary of:
1. The "Plan-Do-Check-Act" cycle
2. Recommended security measures
3. Checks regarding security measures
4. The list of subjects that must in any event be provided for in a processing agreement.

To read the guidelines in Dutch, click here.

Nieuwe beveiligingsrichtlijnen

*Op 19 februari 2013 publiceerde het College Bescherming Persoonsgegevens ("**CBP**") **nieuwe richtlijnen ten aanzien van beveiliging** van persoonsgegevens.*

*Deze "**CBP Richtsnoeren"** vervangen eerdere richtlijnen uit 2001.*

*De Richtsnoeren treden op **1 maart 2013 in werking**. Bedrijven zouden de beveiliging conform een Plan-Do-Check-Act cyclus geregeld moeten hebben en eventuele (bewerkers)overeenkomsten zouden de noodzakelijke elementen moeten bevatten.*

Een bedrijf moet ingevolge de Wet bescherming persoonsgegevens passende technische en organisatorische maatregelen treffen om persoonsgegevens te beveiligen tegen verlies, of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen dienen, rekening houdend met de stand van de techniek, en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te garanderen gelet op de risico's die de verwerking en de aard van de persoonsgegevens met zich meebrengen. De maatregelen dienen er mede op gericht te zijn onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. De CBP Richtsnoeren geven hieraan nadere invulling.

De CBP Richtsnoeren schrijven een "**Plan-Do-Check-Act**" cyclus voor met de volgende stappen:
1. Risicoanalyse
2. Beveiligingsmaatregelen passend bij de risicoanalyse
3. Periodieke controle naleving maatregelen
4. Periodieke evaluatie en aanpassing naar aanleiding van gewijzigde omstandigheden.

Veel bedrijven laten persoonsgegevens verwerken door een **bewerker**. Dit is een externe organisatie die persoonsgegevens alleen in opdracht van en namens het bedrijf verwerkt volgens de instructies van het bedrijf en deze niet voor eigen doeleinden mag gebruiken (voorbeelden zijn het uitbesteden van de salarisadministratie, of hosting). De Richtsnoeren bevatten een lijst met onderwerpen die in een (**bewerkers)overeenkomst** in ieder geval moeten zijn geregeld.

Volgens het CBP wordt over het algemeen een optimale beveiliging bereikt door de informatiebeveiliging in te richten op basis van een **algemene beveiligingsstandaard** zoals de Code voor Informatiebeveiliging en bijvoorbeeld bij de ontwikkeling en het beheer van webapplicaties uit te gaan van de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC. In de Richtsnoeren wordt dan ook steeds verwezen naar de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007.nl).

Voor een samenvatting inzake:
1. Plan-Do-Check-Act cyclus;
2. Aanbevolen beveiligingsmaatregelen
3. Controle maatregelen
4. Lijst met onderwerpen die in ieder geval in een bewerkersovereenkomst moeten zijn geregeld.
klik hier

Om de Richtsnoeren te lezen klik hier.

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