Newsletter GDPR Sensitive personal data

March 22, 2017

This third GDPR newsletter deals with the differences under the Data Protection Directive, implemented by the Dutch Personal Data Protection Act (the DPA) and the General Data Protection Regulation (the GDPR) with regard to the processing of sensitive personal data.

At first glance, the changes with regard to the processing of sensitive personal data under the GDPR appear to be limited. Similar as under the DPA, the processing of sensitive personal data is in principle prohibited and the grounds for processing such data are broadly the same as under the DPA.

What is sensitive personal data?

Under the GDPR personal data that regard one more of the following categories is considered sensitive data:

1. Racial or ethnic origin
2. Political opinions
3. Religious or philosophical beliefs
4. Trade union membership
5. Data concerning health or data concerning a person's sexual life or sexual orientation
6. Genetic data (new)
7. Biometric data if processed to uniquely identify a person (new)

The above categories are broadly similar to those in the DPA, with the exception that sensitive personal data now specifically includes genetic data and biometric data. Further, under the GDPR the processing of photographs is not systematically considered to be a processing of sensitive personal data. Photographs are only considered biometric data when processed through a specific technical means allowing the unique identification or authentication of a natural person.

Exceptions to the prohibition to process sensitive data

Under the GDPR the processing of sensitive data is allowed only if one of the below exceptions apply:

1. The data subject has given its explicit consent. Such consent should be freely given, specific, informed and unambiguous (see our newsletter of February 2017). Note that the processing of medical data of employees by employers (including for drugs or alcohol testing) cannot be based on the consent from the employee. In view of to the hierarchal relationship such consent is not considered freely given.
2. The processing of such data is necessary for employers in the field of employment, social security or social

protection law, in so far as such processing is authorised by Union or Member State law or a collective agreement.

3. The processing is necessary to protect the vital interests of the data subjects or of another person and the data subject is physically or legally incapable of giving its consent (emergency situations).
4. The processing is carried out by a not-for-profit body with a political, philosophical, religious, or trade union aim, provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent.
5. The processing relates to personal data which are made public by the data subject.
6. Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
7. The processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures.
8. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services, on the basis of Union or Member State law or pursuant to a contract with a health professional.
9. The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject.
10. The processing is necessary for archiving purposes in the public interests, statistical, scientific or historical research purposes, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

While the categories of sensitive personal data and the grounds for processing such data broadly replicate those under the DPA, the GDPR brings several changes.

Firstly, paragraphs (b), (g), (h), (i) and (j) above refer to Member State law as the legal basis for the processing, and the GDPR allows that Member States maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.

Consequently, existing differences between Member States in approach on these subjects will likely be upheld and further divergence between Member States may emerge.

The Dutch government recently published its proposal for an Implementation Act. Under this Implementation Act, the conditions for the processing of sensitive personal data remain similar as under the DPA.

Secondly, organisations are obliged to perform a privacy impact assessment (PIA) when the processing of personal data is likely to result in a high risk to the rights or freedom of data subjects. The purpose of a PIA is to identify such high risks and to formulate measures to address these risks. A PIA must be carried out prior to commencing the processing activity.

The GDPR explicitly states that a PIA is mandatory in the case of large-scale processing of sensitive personal data or of personal data relating to criminal convictions and offences (we will discuss the PIA in more detail in one of the following GDPR newsletters).

Thirdly, the large-scale processing of sensitive personal data may require the controller (or processor) to appoint a Data Protection Officer (DPO). We will address the DPO in the a subsequent newsletter, together with the PIA.

Practical recommendations

The entry into force of the GDPR will not substantially affect existing practices regarding the processing of sensitive personal and the changes, at first glance, appear to be limited. However, there are changes which may have an impact on the way organisations must process sensitive personal data. Organisations which process sensitive personal data would therefore do well to review their existing policies and practices and ensure that:

- a PIA is undertaken prior to the large-scale processing of sensitive personal data;
- if sensitive personal data is processed based on consent, the quality of consent meets the new requirements under the GDPR. Note that in employer-employee relationship consent for the processing of (sensitive) data will in principle be regarded as not given voluntarily;
- a DPO is appointed where required;
- the processing of sensitive personal data meets the conditions (including restrictions) imposed by the relevant Member States.

Overview of subjects

January 2017	Territorial scope of the GDPR (Dutch)
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability)
July2017	Rights of Data Subjects (erasure, restriction, object and automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in Employment Context
April 2018	Profiling and Retail
May 2018	Overview

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09

M +31 6 46 37 61 08
marc.elshof@dentons.com