GDPR Update november 2018: Data protection impact assessments (DPIAs)

November 9, 2018

Introduction

In this month's GDPR Update we address an organization's obligation to perform Data Protection Impact Assessments (DPIAs). A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of individuals resulting from the processing of personal data by assessing them and determining measures to address them.

The obligation to perform DPIAs did not explicitly exist under the repealed Data Protection Directive. Together with the introduction of the accountability principle, this new obligation can be seen as a replacement for the system of notifications of processing activities to national supervisory authorities, which proved to be ineffective in ensuring better data protection and was cost inefficient.

Obligation to perform a DPIA

Carrying out a DPIA is not mandatory for every processing activity. An organization, as a controller, is obliged to perform a DPIA if the processing is "likely to result in a high risk to the rights and freedoms of natural persons." The GDPR non-exhaustively lists the following processing activities as likely to result in a high risk:

i. A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
ii. Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; and
iii. A systematic monitoring of a publicly accessible area on a large scale (e.g. through CCTV).

The guidelines of the Article 29 Working Party (the WP29, as replaced by the European Data Protection Board, the EDPB) on DPIAs set out that in most cases a processing activity is likely to result in a high risk if it meets two or more of the following criteria:

1. Evaluating or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" (e.g. determining a credit score, evaluating someone's health, performance at work, or personal preferences or interests).
2. Automated decision making with legal or similar significant effect, such as decisions made by an automated system based on a profile in order to allow or deny a customer's access to a financial product.
3. Systematic monitoring (i.e. processing used to observe, monitor or control data subjects, including data collected

through networks or “a systematic monitoring of a publicly accessible area”), such as CCTV or workplace monitoring systems.
4. Sensitive data or data of a highly personal nature such as health or racial/ethnic data, information about individuals’ political opinions and criminal convictions.
5. Data processed on a large scale (taking into consideration the number of data subjects concerned, the volume of data, the duration or permanence of the processing activity and the geographical scope of the processing activity), such as tracking individuals through a city's public transport system via geolocation.
6. Matching or combining datasets such as combining, comparing or matching personal data from multiple sources.
7. Data concerning vulnerable data subjects (e.g. children, employees, elderly and patients).
8. Innovative use or application of new technological or organizational solutions such as the use of artificial intelligence to make decisions.
9. When the processing in itself “prevents data subjects from exercising a right or using a service or contract.”

As a general rule, the more of these criteria that are met the more likely it is that a processing activity poses a high risk and therefore requires performance of a DPIA.

DPIA lists

Under the GDPR, supervisory authorities are obliged to create and publish lists of specific processing activities that require a DPIA in any case. For an impression of what type of processing activities are on these lists, please see the schedule below.

The Netherlands	Belgium	United Kingdom
Large scale/systematic processing for secret investigation (e.g. private detective companies)	The use of biometric data for unique identification of data subjects in public spaces or in private spaces that are accessible to the public	Processing involving the use of new technologies, or the novel application of existing technologies (including artificial intelligence)
Black lists (e.g. on persons with bad payment habits)	Processing of data that is collected from third parties for the purposes of taking decisions about terminating or denying a service agreement with a natural person	Decisions about an individual’s access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
Large scale/systematic processing for fraud prevention (e.g. by social security institutions)	Processing of special categories of data for other purposes than for which the data was collected, unless the processing is based on the data subject’s consent or if the processing is necessary to fulfill a legal obligation to which the controller is subject	Any profiling of individuals on a large scale
Large scale/systematic processing for credit scoring	Processing by means of an implant and whereby a personal data breach could threaten the physical health of the data subject	Any processing of biometric data
Large scale/systematic processing to assess	Large scale processing of personal data of vulnerable natural persons, such as children, for other purposes than for which the data was	Any processing of genetic data, other than that processed by an individual general practitioner or health

The Netherlands	Belgium	United Kingdom
financial situation	originally collected	professional for the provision of health care direct to the data subject
Large scale/systematic processing of genetic data	Large scale collection of personal data from third parties for the purposes of analyzing or predicting the economic situation, health, personal preferences or interests, reliability or behavior, location or movements of natural persons	Combining, comparing or matching personal data from multiple sources
Large scale processing of health data	Systematic exchange between different controllers of special categories of personal data or personal data of a highly personal nature (such as information about poverty, unemployment, involvement of youth care or social work, household or private activities, location)	Invisible processing, i.e. processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 (providing information to the data subjects) would prove impossible or involve disproportionate effort
Exchange of sensitive data and special category data	Large scale processing of data that is generated through the use of devices with sensors that send data via the internet or another medium (Internet of things-devices, such as smart televisions, smart household appliances, connected toys, smart cities, smart energy meters, et cetera) for the purposes of analyzing or predicting the economic situation, health, personal preferences or interests, reliability or behavior, location or movements of natural persons	Processing which involves tracking an individual's geolocation or behavior, including but not limited to the online environment
Structural and large scale CCTV surveillance of public spaces	Large scale processing and/or systematic processing of telephone, internet or other communication data, metadata or location data traceable to natural persons (e.g. wifi-tracking or processing of travellers data in public transport) when the processing is not strictly necessary for a service requested by the data subject	The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children
Large scale/systematic flexible camera surveillance (e.g. use of dashboard cameras)	Large scale processing of personal data whereby the behavior of natural persons is automatically and systematically observed, collected, recorded or influenced, including for advertising purposes	Where the processing is of such a nature that a personal data breach could jeopardise the (physical) health or safety of individuals
Large scale/systematic employee monitoring		
Large scale/systematic processing of location data		
Large scale/systematic processing of communication data		

The Netherlands	Belgium	United Kingdom
Large scale/systematic processing through internet of things devices		
Systematic and extensive profiling		
Large scale observation and influencing of behaviour		

The EDPB has recently (September 2018) issued opinions on these lists in order to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

From the EDPB's opinions it inter alia follows that:

- the processing of biometric data;
- the processing of genetic data;
- the processing of location data; or
- the processing with the use of innovative technologies;

on its own, is not necessarily likely to present a high risk. However, the processing of such data in conjunction with at least one other criterion from WP29's list (see under "Obligation to perform a DPIA" above) will require a DPIA to be carried out.

The DPIA lists have to be amended in accordance with these opinions (if not amended yet).

Decision not to perform a DPIA

If an organization based on the above factors (WP29 guidance and supervisory authorities' DPIA lists) comes to the conclusion that it is not obliged to perform a DPIA, it should document how it has formed that opinion, to be able to demonstrate GDPR compliance. A decision not to perform a DPIA should not be a one-off decision. Controllers must continuously asses their processing activities to identify when an activity is likely to result in a high risk to the rights and freedoms of data subjects.

How to perform a DPIA

Under the GDPR, the process to perform a DPIA has not been specified. The GDPR allows for data controllers to introduce a framework which complements their existing working practices provided it takes into account the following minimum requirements:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
- An assessment of the necessity and the proportionality of the processing operations in relation to the purposes.

- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address the risks and demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The controller must request advice from the Data Protection Officer (the DPO) when performing a DPIA. The DPO shall also monitor performance of the DPIA in accordance with the GDPR. Where appropriate, the controller should consider seeking the views of the data subjects on the intended processing.

A single DPIA may be undertaken in respect of similar data processing operations that present similar risks. This might be the case where similar technology is used to collect the same sort of data for the same purposes (for example the use of CCTV in multiple locations of the same company if the CCTV is used in the same way).

When to perform a DPIA

According to the WP29, a DPIA should be seen as a decision-making tool concerning the processing. A DPIA should therefore be carried out “prior to the processing”. It is advisable to start the DPIA as early as possible in the design and proof of concept phases of the processing operation.

Further, the WP29 emphasizes that carrying out a DPIA is a continual process and not a one-time exercise. A DPIA should be continuously reviewed and regularly reassessed. The Dutch supervisory authority for example suggests reassessing a DPIA at least every three years, and the Belgian supervisory authority suggests a reassessment every two years. If in the meantime changes occur in the risk level of the processing activities, a reassessment should be performed at the time of these changes.

The requirement to carry out a DPIA also applies to existing processing operations.

Consulting the supervisory authority

If a DPIA identifies a high risk, and an organization is not able to take measures to reduce the risk, that organization should consult the competent supervisory authority. If the supervisory authority is of the view that the processing activities will violate the GDPR, the supervisory authority will provide a written advice to the controller within eight weeks. The advice may entail that measures should be taken to comply with the GDPR or that the proposed processing operation may not be started. Whether in practice these prior consultations will often be requested remains to be seen, as controllers will likely be reluctant to inform the supervisory authority about a high risk processing for which it cannot find mitigating measures. Further, the response from the supervisory authority is predictable: “such processing violates the GDPR, so don’t do it.”

Practical recommendations

Organizations should assess whether they are obliged to perform DPIAs (e.g. by conducting a DPIA gateway assessment). If the organization decides that it does not deem it necessary to perform a DPIA, it should document the ratio behind such a decision in order to demonstrate that it is based on the relevant factors. It is important that a controller continuously assesses its processing activities to determine whether a decision not to perform a DPIA should be revised.

If an organization comes to the conclusion that it should perform a DPIA, it should make sure that it meets the minimum requirements. With regard to the performed DPIA’s, it is best if the organization designs a process to

periodically reassess them (e.g. once every two or three years). In any case a reassessment should take place if changes occur in the underlying processing activity(ies).

Organizations should create awareness within the organization with regard to the processing of personal data and, in particular, the obligation to perform DPIAs. The relevant individuals (e.g. key personnel within the IT team, HR, procurement, product development) should be made aware of the organization's DPIA policy. The DPO, or other individual responsible for GDPR implementation within the organization, should be responsible for creating this awareness.

Please click here to subscribe to our monthly updates on the GDPR.

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, objectand 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 the Employment Context
April 2018	Profiling and Retail
May 2018	Overview
October 2018	Overview of developments since May 25, 2018
November 2018	Data Protection Impact Assessments (DPIAs)

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Celine van Es
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com