First Guidance on GDPR Published by the EU Data Protection Regulators

D&I Alert

20 December 2016

» Data Protection, Marketing & Consumers

FIRST GUIDANCE ON GDPR PUBLISHED BY THE EU DATA PROTECTION REGULATORS

On 15 December 2016, the Article 29 Data Protection Working Party (the "WP29") published the first guidance on three topics relating to the interpretation of the General Data Protection Regulation (the "GDPR").

BACKGROUND

The European Union General Data Protection Regulation (EU) 2016/679 ("GDPR") entered into force on 24 May 2016 and shall apply from 25 May 2018.

The full effects of the GDPR are yet to be clarified by the WP 29's (the group of regulators which will later form the European Data Protection Board) guidance. Such guidance will be issued on various topics requiring more specific instructions and interpretations. We at D&I will keep you posted on the developments as they unravel and are happy to help with any questions you may have regarding the GDPR and its effects.

During its meeting held last week, the WP29 completed guidelines on:

- Data Portability (full guidelines here);
- Data Protection Officers (full guidelines here); and
- Lead Supervisory Authority (full guidelines here).

You can find the press release published on 15 December 2016 here.

We have summarised the most important aspects introduced by the guidelines and their effects on businesses.

GUIDELINES ON THE RIGHT TO DATA PORTABILITY

How is your business affected?

According to D&I's review, in its guidance, the WP29 adopts a very broad interpretation of the right to data portability. In addition to the data provided actively by the data subject, data generated by or collected from the activities of the data subject (such as location data or heartbeat tracked by wearable devices) fall within the scope of the right to data portability. The controller is not obliged to ensure that the receiving controller has the right to process the data, but it

should provide the data subjects with a direct download opportunity and allow them to transmit the data to another controller directly.

What is the right to data portability?

Article 20 of the GDPR provides the data subject with a new right to data portability, which allows data subjects to receive the data they have provided to the controller in a machine readable format and to transmit the data to another controller upon the data subjects' request.

According to the GDPR, the right to data portability only applies if the processing is based on either consent or a contract, and is carried out by automated means.

What kind of data is covered?

The WP29 adopts a **broad interpretation** of the right to data portability. Data actively provided by data subjects (e.g. name in the user profile) and data generated from the use of services or devices (e.g. search history, location data and raw data such as heartbeat collected by wearable devices) are in the scope of the right. The right does not cover data "*exclusively generated by the data controller such as a user profile created by analysis of the raw smart metering data collected*".

The issued interpretation does not affect the implementation of other data subject rights, such as the right of access.

Although potential risks to intellectual property rights and trade secrets should be assessed by the controller, potential business risks do not constitute a right to refuse to transfer data. However, the data may be transferred in a form that does not release such trade secrets.

What are the receiving controllers' obligations?

The **receiving controller** has to ensure that it has the right to process the data in question and that the data is relevant with regard to the receiving controller's processing activities. It is recommended that the receiving controller provide the data subject with information on which personal data is relevant, so that the data subject may then provide only such relevant data to the receiving controller. The receiving controller should also note that the data may include personal data of other data subjects and that it may not use such data.

How to provide the data?

Controllers should provide the data subjects with a direct download opportunity and allow them to transmit the data to another controller directly (e.g. through an API). **The transmission of the data does not trigger the obligation to erase the data.**

The data must be structured and machine-readable (i.e. not in .pdf-format) and include as much metadata as possible. Controllers are not obliged to

adopt compatible systems in order to meet this requirement, but the aim is to produce interoperable systems.

> GUIDELINES ON DATA PROTECTION OFFICERS

How is your business affected?

*According to D&I's review, the WP29 clarifies the obligation to appoint a Data Protection Officer ("**DPO**"). In addition, the WP29 seeks to clarify concepts that were left open in the GDPR, such as, "public authority", "core activities", "large scale" and "regular and systematic monitoring". Finally, the WP29 further clarifies on the position and tasks of the DPO. The WP29 clearly reaffirms that the DPOs will not be personally responsible for non-compliance with the GDPR.*

What is a DPO?

The GDPR is based on the accountability principle which places the DPO in the centre of the new legal framework. The appointment of a DPO is mandatory for certain controllers and processors but the WP29 encourages companies to designate a DPO on a voluntary basis as well. Appointing a DPO will help ensure compliance with legal requirements and is likely to become a competitive advantage for businesses. The guidelines further define the position and role of the DPO, but we will not touch upon the details in this Alert.

What concepts does it clarify?

In addition to public authorities, private organisations carrying out public tasks (e.g. public transport services, water and energy supply, public service broadcasting, public housing) should designate a DPO. The tasks of the designated DPO should cover all processing activities (e.g. management of employee database), not only those related to the performance of a public task.

Companies' **core activities** are the key operations necessary to achieve the controller's or processor's goals. For example, a hospital's core activity is to provide healthcare. In order to do so they process health data, such as patients' records. Therefore, the processing of such data should be considered a hospital's core activity. This results in an obligation to appoint a DPO. Ancillary functions, such as paying employees or having standard IT support activities do not give rise to an obligation to appoint a DPO.

The WP29 clarifies the concept of "**large-scale processing**" by providing a list of activities that includes, for example: a hospital processing patient data during the regular course of its business, processing travel data (e.g. tracking via travel cards), processing real time geo-location data of customers of an international food chain for statistical purposes, an insurance company or bank processing customer data during the regular course of its business, processing of personal data for behavioural advertising by search engines, and telephone or internet service providers processing personal data

(content, traffic, location). If a company does large-scale processing it must appoint a DPO.

The concept of "**regular and systematic monitoring**" is not limited to the online environment. The WP29 provides a list of examples of regular and systematic monitoring: operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment; location tracking (e.g. by mobile apps); loyalty programs; behavioural advertising; monitoring wellness, fitness and health via wearable devices; CCTV; connected devices (e.g. smart meters, smart cars, home automation); etc. If a company carries out regular and systematic monitoring it must appoint a DPO.

How many DPOs in your Group of Companies?

Article 37(2) of the GDPR allows for a group of companies to appoint a single DPO provided that he or she is "*easily accessible from each establishment*". The WP29 further clarifies that this means that the DPO must be accessible as a contact point with respect to data subjects, the supervisory authority and internally within the organisation.

In order to ensure availability, the DPO must be able to communicate with the data subjects and the supervisory authority in the **same language** used by the supervisory authority and the by the data subjects concerned. Furthermore, the DPO must be personally available whether physically on the same premises as employees or via a secure means of communication.

Can you appoint an external DPO?

Yes. The DPO may be a staff member of the controller or the processor (internal DPO) or fulfil the tasks on the basis of a service contract (external DPO). The external DPO must fulfil all relevant requirements of the GDPR. The WP29 recommends assigning a single individual as a lead contact and person "in charge" for each client when a team of individuals is working to effectively carry out the tasks of the DPO.

> GUIDELINES ON IDENTIFYING A CONTROLLER'S OR PROCESSOR'S LEAD SUPERVISORY AUTHORITY

How is your business affected?

The WP29 reassured that there can be more than one lead supervisory authority in cases where the controller has separate decision making centres in different countries for different processing activities. The WP29 further clarifies that a company whose decisions are taken exclusively outside of the territory of the EU should designate an establishment to act as its main establishment within the EU for data protection matters. Finally, the WP29 provides further criteria on determining when the data processing 'substantially affects' data subjects in other Member States and can thus constitute cross-border data processing.

What is a lead supervisory authority?

The GDPR introduces a one stop shop -system, which means that the lead supervisory authority will supervise all cross-border data processing activities of the controller or processor, and act as its sole interlocutor. According to the GDPR, the lead supervisory authority is the supervisory authority of the controller's or processor's main or single establishment in the EU. Identifying a lead supervisory authority is relevant where a controller or a processor is carrying out cross-border processing of personal data.

When does data processing substantially affect data subjects in other Member States?

Processing can be considered cross-border processing if it is 'likely to substantially affect data subjects'. In order to '**substantially affect**' data subjects, the processing must have an impact on the data subjects. The WP29 points out that the interpretation will be case-specific taking into consideration the context and the purpose of the processing as well as the type of data.

How to identify the lead supervisory authority?

The lead supervisory authority is the supervisory authority of the controller's or processor's main or single establishment in the EU (i.e. the place of its central administration where decisions concerning the processing activities are taken). The GDPR does not offer a solution for situations where decisions are made exclusively outside of the EU. The WP29 suggests that in order to benefit from the One-Stop-Shop -system, **the company should designate an establishment to act as its main establishment within EU**.

> LOOKING FORWARD

The WP29 welcomes additional comments from the stakeholders on the guidelines until the end of January 2017. In addition, the WP29 announced that more guidelines will follow, namely on Data Protection Impact Assessments and Certification. D&I will provide further insight on these when published.

As the GDPR leaves some of the issues to be decided upon by the member states, not all issues are clarified on the EU level. The implementation process in Finland is under way and is lead by the Finnish Ministry of Justice. The Ministry has placed a working group to aid it in the process. In 2015, the Finnish Ministry of Justice assigned D& I to prepare a report on the impact of the Regulation on companies established in Finland.

We at Dittmar & Indrenius are happy to help with any questions you may have regarding the GDPR and its effects, and will keep you posted on the implementation process and the further clarifications from the European Data Protection Authorities.

Jukka Lång
Partner, Head of Data Protection, Marketing
& Consumers

jukka.lang@dittmar.fi
+358 9 6817 0118
+358 40 719 4317

Ricardo Gomes
Associate

ricardo.gomes@dittmar.fi
+358 9 6817 0174
+358 40 935 5105

Tuomas Haavikko
Associate

tuomas.haavikko@dittmar.fi
+358 9 6817 0136
+358 44 582 8260

Dittmar & Indrenius renders insightful and comprehensive advice to demanding corporate clients. We focus on creating exceptional added value. Our ambition is to be the best law firm partner for our clients.
www.dittmar.fi

Dittmar & Indrenius, Pohjoisesplanadi 25 A, FI-00100 Helsinki
Tel: +358 9 681 700
www.dittmar.fi