GDPR Update: One Stop Shop

January 19, 2018

Introduction

In this first GDPR Update of 2018, we address the One Stop Shop mechanism. The One Stop Shop mechanism means that, as a main rule, organisations carrying out cross-border personal data processing activities will only have to deal with one supervisory authority in the future. This supervisory authority is called the 'lead supervisory authority'.

The Directive 95/46/EC does not provide a One Stop Shop mechanism. In practice, this means that it is possible that organisations with several establishments in the European Union (the EU) are confronted with inconsistent decisions by various local supervisory authorities. The One Stop Shop principle intends to change this situation. From 25 May 2018, certain organisations may benefit from the fact that they will mainly have to deal with only one supervisory authority. This should lead to a uniform application of the GDPR and consistent GDPR related decisions by supervisory authorities.

Cross-border processing

The One Stop Shop mechanism only applies in cases of cross-border data processing activities. The GDPR defines a cross-border processing as:

i. the processing of personal data which takes place in the context of the activities of establishments in more than one EU member state of a controller or processor in the EU where the controller or processor is established in more than one EU member State; or
ii. as processing of personal data which takes place in the context of activities of a single establishment of a controller or processor in the EU but which substantially affects or is likely to substantially affect data subjects in more than one EU member State.

The GDPR does not define "substantially affects". The mere fact that a specific personal data processing affects a large number of individuals in more than one EU member state, does not necessarily mean the processing substantially affects these individuals. Supervisory authorities have to take into account the context of the processing, the type of personal data and the purpose of the processing. The Article 29 Working Party (the WP29) has formulated a number of circumstances that supervisory authorities should take into account where interpreting the criterion of "substantially affects". According to the WP29, it can be relevant whether the processing:

- causes, or is likely to cause, damage, loss or distress to individuals;
- has, or is likely to have, an actual effect in terms of limiting rights or denying an opportunity;
- affects, or is likely to affect individuals' health, well-being or peace of mind;

- affects, or is likely to affect, individuals' financial or economic status or circumstances;
- leaves individuals open to discrimination or unfair treatment;
- involves the analysis of the special categories of personal data or other intrusive data, particularly the personal data of children;
- causes, or is likely to cause individuals to change their behaviour in a significant way;
- has unlikely, unanticipated or unwanted consequences for individuals;
- creates embarrassment or other negative outcomes, including reputational damage; or
- involves the processing of a wide range of personal data.

Lead supervisory authority

The 'lead supervisory authority' is the authority with the primary responsibility for dealing with cross-border data processing activities, for example, when a data subject makes a complaint about the processing of his or her personal data. The lead supervisory authority will coordinate any investigation and will be entitled to involve other 'supervisory authorities concerned' in such investigation.

Identifying the lead supervisory authority depends on determining the location of the 'main establishment' or 'single establishment' of the data controller or processor in the EU. If the organisation has only one establishment in the EU, the designation of the lead supervisory authority is relatively straightforward. However, identifying the main establishment of an organisation with more than one establishment in the EU will be more complex. Below, we address some examples.

Main establishment in the EU

The location of the central administration

The GDPR defines a controller's main establishment as the place where the controller has its central administration in the EU. The central administration in the EU is the place where decisions about the purposes and means of the personal data processing are taken. To be able to determine which supervisory authority is the lead supervisory authority, it will be essential for organisations to determine where the decisions regarding the purposes and means of the processing are taken.

The location of the central administration is not in the EU

If the decisions about the purposes and means of the processing are not taken within an establishment of the controller in the EU (i.e. the criterion of central administration does not apply), the controller will have to identify where the effective and real exercise of management activities, that determine the main decisions as to the purposes and means of processing through stable arrangements, takes place. The GDPR explicitly sets out that the presence and use of technical means and technologies for processing personal data or processing activities does not as such constitute a main establishment. Therefore, these are not determining factors for a main establishment. The following questions, as formulated by the WP29, can help determine the location of a controller's main establishment in cases where it is not the location of its central administration in the EU:

- Where are decisions about the purposes and means of the processing given final 'sign off'?

- Where are decisions about business activities that involve data processing made?
- Where does the power to have decisions implemented effectively lie?
- Where is the Director (or Directors) with overall management responsibility for the cross border processing located?

We note that the aforementioned questions can also be relevant in determining the location of controller's main establishment in cases where all the establishments of the data controller are located in the EU, but none of these establishments can be identified as the location of the central administration. This can occur with decentralised multinational organisations.

'Forum shopping' is prohibited. If, for example, an organisation holds the view that its main establishment is located in the Netherlands, but no management activities actually take place in that establishment and/or no decisions regarding the processing of personal data are made in that establishment, supervisory authorities will determine which supervisory authority is the lead supervisory authority on the basis of objective criteria and concrete evidence. Supervisory authorities may dispute an organisation's appointment of its main establishment (and thereby the lead supervisory authority). Taking into account the GDPR's principle of accountability, we recommend properly recording considerations regarding the above.

Data processors

Data processors may also benefit from the One Stop Shop mechanism. A processor's main establishment will be the place of its central administration in the EU. If the data processor has no central administration in the EU, the main establishment will be the location where its main processing activities take place.

However, in matters involving both the controller and the processor, the lead supervisory authority of the controller will qualify as the competent lead supervisory authority. In such cases, the supervisory authority of the processor will be a 'supervisory authority concerned' that has to participate in the cooperation procedure. In practice, this will mean that - also under the GDPR - processors providing services to various data controllers established in more than one member state (e.g. cloud service providers) will still have to deal with multiple supervisory authorities.

Organisations located outside the EU

The One Stop Shop mechanism only applies to organisations with one or more establishments in the EU. The mere presence of a representative of the organisation in the EU is insufficient in this respect. If the organisation has no establishments in the EU, but its processing activities are covered by the GDPR's territorial scope, that organisation cannot apply the One Stop Shop mechanism. Organisations with no establishments in the EU, will have to deal (through their representatives) with the local supervisory authorities in every EU member state it processes personal data.

Conclusion

Organisations carrying out cross-border processing activities that would like to benefit from the One Stop Shop principle should carefully determine the location of their main establishment in the EU. We recommend making an overview of the various establishments and assessing in which establishment (or establishments) the decisions regarding the purposes and means of the personal data processing are taken and whether or not this entity is established in the EU. Based on such assessment and with the guidance of the WP29 as set out in this GDPR

Update, organisations will be able to identify which establishment is its main establishment. By recording the considerations organisations make in this respect, organisations will be able to substantiate their decisions regarding the lead supervisory authority in potential disputes with supervisory authorities.

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, 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