GDPR Update: Sanctions

February 23, 2018

Introduction

In this GDPR update, we address the sanctions supervisory authorities may impose on organisations that are non-compliant with the GDPR.

Significant administrative fines and other corrective powers of the supervisory authorities are a central element of the new enforcement regime introduced by the GDPR. From 25 May onwards, data controllers and data processors have increased responsibilities to ensure that personal data will be protected effectively. If organisations do not comply with these responsibilities, it may result in the application of sanctions by supervisory authorities.

To ensure a consistent and high level of protection for individuals, the level of protection should be equivalent in all EU member states. In cross border cases, consistency on the sanctions can be achieved through the one-stop-shop mechanism and, to a certain extent, through the cooperation of supervisory authorities under the GDPR's consistency mechanism. The GDPR intends to avoid that different corrective measures will be applied by the supervisory authorities in similar cases, although supervisory authorities remain independent in their choice of the specific corrective measure.

Corrective measures

In case of an infringement of the GDPR, the competent supervisory authority will identify the most appropriate corrective measure(s) to address the infringement. The supervisory authority has various tools (i.e. corrective powers) in this respect. Potential sanctions include more than just administrative fines. To address an organisation's non-compliance with the GDPR, the competent supervisory authority may:

a. Issue warnings to organisations that intended processing operations are likely to infringe provisions of the GDPR;
b. Issue reprimands to organisations where processing operations have infringed provisions of the GDPR;
c. Order organisations to comply with data subject's requests to exercise his or her rights;
d. Order organisations to bring processing operations in compliance with the provisions of the GDPR;
e. Order the controller to communicate a personal data breach to the affected data subjects;
f. Impose a temporary or definitive limitation on a personal data processing, including a ban on such processing;
g. Order the rectification or erasure of personal data or restriction of processing, and the notification of such actions to recipients to whom the personal data has been disclosed;
h. Withdraw a certification or order a certification body to withdraw a certification, or order a certification body not to issue certification if the requirements for the certification are not or no longer met;
i. Order the suspension of data flows to a recipient in a third country or to an international organisation; and/or
j. Impose an administrative fine, in addition to, or instead of the corrective measures referred to above, depending on

the circumstances of each individual case. We will address the fines in more detail below.

Each measure taken by a supervisory authority must be appropriate, necessary and proportionate, yet at the same time dissuasive. The competent supervisory authorities have to make case-by-case assessments, based on all circumstances of the case.

If, for example, the breach is a minor infringement of the GDPR only, a reprimand may be issued instead of an administrative fine.

Administrative fines

While the current data protection directive (Directive 95/46/EC) only states that sanctions have to be formulated by the EU member states, the GDPR sets out the administrative fines for non-compliance. When imposing an administrative fine, a supervisory authority is obliged to take into account all circumstances of the case. This includes the following circumstances:

- The nature, gravity and duration of the infringement, the number of individuals affected, the purpose of the processing, the level of damage suffered by affected individuals and the duration of the processing;
- The intentional or negligent character of the infringement;
- Any action taken by the organisation to mitigate the damage suffered by data subjects (i.e. reducing the consequences of the breach);
- The degree of responsibility of the organisation, taking into account any technical and organisational measures it has taken;
- Any relevant previous infringements by the organisation;
- The degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- The categories of personal data affected by the infringement (any special of particularly sensitive categories of data?);
- The manner in which the infringement became known to the supervisory authority (in particular whether the organisation notified the infringement itself, e.g. in case of a data breach);
- Compliance with previously ordered measures against the organisation regarding the same subject matter;
- Adherence to approved codes of conduct or approved certification mechanisms. If these contain adequate sanctioning provisions they may be effective, proportionate and dissuasive enough, limiting the need for a supervisory authority to impose additional measures; and
- Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided from the infringement.

With respect to the application and setting of administrative fines, the Article 29 Working Party recently published guidelines in which it provides guidance regarding the interpretation of the circumstances listed above.

Two levels of maximum fines

Under the Dutch Personal Data Protection Act (the DDPA), the Dutch Supervisory Authority (Autoriteit Persoonsgegevens) has the authority to impose fines on organisations infringing the DDPA (but only since 1 January 2016). Currently, administrative fines amount to a maximum of €820,000 per infringement. Only in case of intent or negligence may the Dutch Supervisory Authority immediately impose a fine. In other cases, the Dutch Supervisory Authority must issue a binding instruction before imposing a fine. The Dutch Supervisory Authority published guidelines on administrative fines under the DDPA, providing details on the level of fines in specific cases.

The GDPR sets out two levels of maximum fines that may be imposed in case of infringements. Depending on the infringed provision, administrative fines may amount to a maximum of €20,000,000, or, when this amount is higher, 4% of the total worldwide annual turnover of an organisation. The second tier of fines is up to a maximum of €10,000,000 or 2% of the total worldwide annual turnover. These amounts are maximum amounts, which means that supervisory authorities are empowered to assess lower, but not higher fines.

The higher tier of fines is limited to the most serious violations of the GDPR by organisations, including infringements relating to the:

- o Basic principles of processing, including conditions for consent;
- Rights of data subjects; and
- Transfers of personal data to third country recipients.

Violations of most other provisions are subject to the second tier of fines. These fines cover infringements related to:

- Consent mechanisms for the processing of personal data relating to children;
- A failure to implement data protection 'by design and by default' ;
- The obligation to maintain records of processing activities;
- A failure to cooperate with the supervisory authority;
- The security of processing data;
- Reporting personal data breaches to the supervisory authority;
- Communication of a personal data breach to the data subject;
- Data Protection Impact Assessments; and
- The designation of Data Protection Officers.

Enforcement and judicial remedies

The competent supervisory authority has the authority to monitor and enforce compliance with the GDPR of its own accord (e.g. perform audits). However, in practice, supervisory authorities will probably be responding mostly to complaints of data subjects (a right data controllers should explicitly make data subjects aware of prior to the processing of their data, and also when they respond to data subject's access requests) or coverage in the media.

In case of a legally binding decision of a supervisory authority (e.g. an imposed fine), organisations must have the right to an effective judicial remedy against such decision. Under Dutch law, organisations have the right to object to a supervisory authority's decision addressed to them and subsequently appeal before the administrative courts.

Conclusion

The powers of the supervisory authorities to impose substantial fines or other sanctions for non-compliance with the GDPR underline the importance of preparing your organisation for the GDPR. These fines and penalties encourage accountability.

However, we believe that the fear for significant administrative fines or other sanctions should not be the main motivator for organisations to comply with the GDPR. Compliance with the GDPR should primarily be based on organisations' intrinsic motivation to protect individuals (e.g. its employees) and to bind important customers (both B2B and B2C) by creating trust that personal data is processed fairly and in a transparent manner.

Furthermore, it is not to be expected that (maximum) administrative fines will be imposed on organisations immediately and organisations that are already well underway with the implementation of the GDPR on 25 May 2018, will likely face other corrective measures first.

The above does of course not mean that the 25 May 2018 deadline should be ignored, and companies that are not yet ready for the GDPR should focus on their high-risk processing activities first.

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 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