GDPR Update - GDPR in the Netherlands: one year after

May 27, 2019

Introduction

It has been one year since the GDPR became applicable.

In the run-up to May 25, 2018, there was much public debate surrounding the implementation of the new privacy legislation. The abbreviation 'GDPR,' the date of May 25, 2018, and the prospect of €20 million fines had been all over the media, leading to anxiety within many organizations, from globally operating enterprises to local sports clubs.

A large part of the public debate focused on potential enforcement activities by supervisory authorities. Organizations seemed most worried about being fined and the accompanying negative publicity risks. This anxiety was strengthened by the silence from the Dutch Data Protection Authority (DDPA) and other local supervisory authorities over their envisaged enforcement strategy.

From May 25 onwards, however, the DDPA became more transparent about its supervisory and enforcement strategy in the Netherlands, not only on paper but also in practice.

In this contribution, we briefly discuss the activities of the DDPA over the past 12 months.

DDPA's Supervisory Framework 2018-2019

The day the GDPR became applicable, the DDPA published its Supervisory Framework 2018-2019, setting out the DDPA's ambitions, core values and supervisory goals for the relevant period.

The DDPA set itself three supervisory goals for 2018-2019:

i. encouraging GDPR compliance;
ii. supervising GDPR compliance; and
iii. risk-based supervision of GDPR compliance.

For 2018-2019, the DDPA sees the first goal (i.e. encouraging GDPR compliance) as the most important. As part of encouraging GDPR compliance, the DDPA inter alia deems it necessary to provide guidance on GDPR interpretation and implementation. Examples of such guidance over the past year include the organization of a seminar for data protection officers (DPOs), and the provision of practical guidance through its website, for example regarding the implementation and structuring of privacy policies and data breach documentation.

According to the DDPA, following up on and responding to data subjects' complaints also contributes to encouraging GDPR compliance. The DDPA is particularly interested in recurring complaints relating to the same processing

activity of a specific controller. At the end of 2018, the DDPA had received over 11,000 complaints, which was more than expected. Complaints primarily related to data subjects not being able to exercise their rights or being frustrated in exercising their rights, or to data subjects receiving (tele)marketing communications from parties to whom they did not provide their data.

Data subjects tend to direct their initial complaints at the organization itself, instead of approaching the supervisory authority. It is our experience that organizations should take data subjects' complaints seriously, and should respond to these complaints with due care. Correspondence with the data subject may (and likely will) be disclosed by the data subject to the DDPA at a later stage. When (informally) investigating the complaint, the DDPA will take into account, and appreciate, a cooperative approach by the controller.

With its second goal (i.e. supervising GDPR compliance), the DDPA focuses on compliance with, in particular, the accountability principle: organizations should be able to demonstrate GDPR compliance. Although having the right documents in place does not necessarily constitute compliance, the DDPA considers it an indication of the organization having given thought to the important aspects of the GDPR and taking its privacy obligations seriously.

To establish if organizations comply with the GDPR's accountability principle the DDPA commissioned randomly selected organizations to provide the DDPA with certain information. In this context, the DDPA undertook investigations into various governmental bodies and healthcare institutions on their appointment of a DPO. The DDPA also undertook investigations into some larger private companies in different sectors, to establish if they implemented a register of processing activities and entered into processing agreements with their data processors. Later DDPA research focused on the existence of privacy policies within political parties, and the existence of compliant data breach registers within government organizations. Where the DDPA established that an organization could not (adequately) respond to the DDPA's request, the organization was granted a remedy period to become compliant.

The third goal of the DDPA is a risk-based supervision of GDPR compliance, focusing on processing activities that imply large risks, for example because of the nature of the personal data processed, or the nature or amount of the data subjects involved. The DDPA therefore primarily concentrates on personal data processing by the government and governmental bodies, healthcare institutions and organizations trading in personal data. Additionally, organizations processing significant amounts of financial data have priority.

The first (publicly known) investigations of the DDPA reflect the priorities of the DDPA. Examples of such investigations include:

- An investigation into the Royal Dutch Lawn Tennis Association, which had been accused of selling personal data to third party sponsors. Members of the association apparently lodged multiple complaints with the DDPA regarding this practice;
- An investigation into the Dutch Tax Authority, which had been accused of unlawfully processing special category data, including nationality, in the context of the Dutch Tax Authority's investigations into fraud with childcare allowance; and
- An investigation into various websites, regarding the placing of cookies and collection of consent.

DDPA's Administrative Fines Policy

In March 2019, the DDPA published its revised policy on the calculation of administrative fines for violations of the GDPR and Dutch GDPR Implementation Act (the Fines Policy).

Broadly speaking, in its Fines Policy, the DDPA has determined four categories of fines. Each fine category is

associated with a certain bracket; the purpose of the bracket is to assist the DDPA in maintaining proportional fines to organizations violating the privacy rules, while also establishing a “starting point” or a base penalty. Each fine category has a starting point and a cap; fines may be either decreased or increased depending on the relevant factors that determine the severity of the infringement. The relevant factors align with the general conditions for imposing administrative fines as set out in article 83 GDPR.

The DDPA distinguishes between the following categories of fines:

Category	Fine Bracket (EUR)	Base Penalty (EUR)
I	0 - 200,000	100,000
II	120,000 - 500,000	310,000
III	300,000 - 750,000	525,000
IV	450,000 - 1,000,000	725,000

The GDPR provisions are divided into the four categories. For example, category IV fines include non-compliance with Article 9 GDPR (prohibition to process special category data) and non-compliance with Article 22 (data subject’s right not to be subject to individual automated decision-making).

The standard penalties determined by the DDPA, are relatively low compared to the maximum penalties under GDPR. However, in cases where the DDPA finds that the penalty set in the Fines Policy is not sufficient or appropriate for the infringement, the DDPA is authorized to impose stricter fines as provided for under the GDPR.

Final Remarks

The DDPA’s visibility increased significantly over the past months and it seems–though still understaffed–they are getting up to speed.

Comparing the DDPA’s Supervisory Framework 2018-2019 to its supervisory and enforcement actions in practice, we may conclude that the Supervisory Framework 2018-2019 provides reliable insights into the DDPA’s supervisory activities, although it remains authorized to undertake enforcement actions outside the Supervisory Framework 2018-2019.

In 2018, the DDPA primarily focused on the implementation of, and advising on, the GDPR. It aimed to assist and guide organizations through the rapidly changing privacy law landscape. However, according to its own statements, the DDPA’s focus has started to shift towards persistent enforcement. This is in line with our recent experience with the DDPA.

We are curious to see what this will bring for the rest of 2019 and the coming years.

Happy GDPR anniversary!

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