AUTORITEIT
PERSOONSGEGEVENS

Data Protection Authority Supervisory Framework

Principles for supervision, 2018-2019

1. Introduction

1.1 Future-proofing the protection of personal data

We live in a data-driven world where data-processing companies wield great power, personal data is worth a lot of money, and all sectors of the economy analyse big data. Technology is developing more quickly than ever, a trend that brings potential benefits for all – not only businesses and public authorities, but also individuals who can use new products and services. Protecting personal data is essential in an age of continuous technological development and increasing dependence on digital services. And globalisation means that the processing of personal data is not confined within the Netherlands' borders. In this social context it is vital for people to be able to control what happens to their personal data.

Public authorities and businesses process personal data that is combined in ever-changing ways. Often people are unaware this is taking place. Innovative products and services offer them convenience. But innovation must not be pursued at the cost of the fundamental right to protection of personal data. People therefore need to be able to maintain control over their digital footprint. This is a major challenge in today's world, but it is the only way to ensure people can continue to make decisions freely.

New EU legislation on privacy will come into force on 25 May 2018: the General Data Protection Regulation (GDPR) and the Directive on the protection of personal data processed for the purposes of the investigation and prosecution of criminal offences. This new legislation entails far-reaching changes to the protection of personal data, which also affect supervision and supervisory authorities. The legislation bolsters the privacy rights of all EU residents, imposes stiffer requirements on organisations, and gives European privacy regulators greater powers to take action. The Data Protection Authority (DPA) has made internal organisational changes to facilitate the effective implementation of this new legislation. This effort included drafting a new supervisory framework setting out the DPA's mission and ambitions, the core values to which it adheres in performing its tasks, and the areas on which it intends to focus.

1.2 Mission

We have formulated the following mission based on our statutory remit:

The Data Protection Authority is the independent supervisory body in the Netherlands that fosters and monitors the protection of personal data.

The DPA **fosters** acceptance of responsibility by public authorities, businesses and individuals for the protection of personal data. We do this by informing them of the rules and the risks. We explain to people what their rights are and provide legislators with solicited and unsolicited advice on legislation relating to the processing of personal data. We also encourage organisations to use privacy-friendly systems and processes. We **monitor** compliance with the rules by conducting independent investigations into possible breaches. We do this on our own initiative or in response to complaints. If necessary, we take enforcement action. We work with other European privacy regulators, because we have to respond to both national and international developments. This involves making choices about our role and the most effective approach in each situation. In doing so, our central concern is always the people concerned and the extent to which their fundamental rights have been violated.

1.3 Ambitions

The DPA has formulated three ambitions which define how it intends to fulfil its mission.

1. The Data Protection Authority works to ensure that the value to society of protecting personal data is viewed as self evident

The DPA works to ensure that the importance of a high level of protection for personal data is viewed as self evident. More specifically we aim to stimulate public debate about protecting the fundamental right to the protection of personal data. To this end we work together and enter into dialogue with stakeholders to identify, discuss and if possible devise solutions to problems and risks. We also place relevant issues on the public agenda and actively disseminate information about the resolution of complaints, advisory opinions on legislation, and relevant decisions.

2. The Data Protection Authority is aware of the latest developments and is proactive where the protection of personal data is at risk

The DPA is a knowledge-driven and risk-oriented authority that maintains close ties with other actors in its field. We actively seek contact with people and organisations, participate in the public debate and are aware the issues that are of concern to the public at large. Through our contact with industry bodies, other organisations, public authorities and businesses, we acquire knowledge from outside organisations and they in turn learn from us. We take a proactive approach by offering services, providing information, help and support, and empowering people by giving them tools that allow them to exercise their rights vis-à-vis organisations. Our point of departure is the responsibility borne by people and organisations themselves. We encourage organisations to handle personal data in a proper and accountable manner. We analyse the information derived from systemic supervision, as well as the signals, reports and complaints we receive, with a view to identifying trends and risks. This approach enables us to proactively make our own decisions regarding policy and investigations, rather than simply responding to events.

3. The Data Protection Authority assumes an active role in the development of European rules and cooperation with other European supervisory authorities

International cooperation is not only an ambition; under the GDPR it is a requirement. The DPA has long fulfilled an important role in cooperation between privacy regulators and will continue to do so under the new legislation. We aim to increase privacy protection across the EU and we handle complaints from people in all EU countries about businesses that are established or provide services in the Netherlands. In the event of a possible breach of the protection of personal data of people in the Netherlands by a business based in a different EU country, we actively seek to work with our European partners. For example, we carry out joint investigations and coordinate enforcement measures. We also actively participate in international collaborative forums of privacy regulators, and we pass on the knowledge we gain through these activities to people and organisations in the Netherlands.

1.4 Core values

The DPA is guided by four core values: independence, openness, expertise and effectiveness.

Independence

The Data Protection Authority is an independent supervisory body that is not influenced by businesses or public authorities. We take account of the interests of others, but in so doing we maintain our independence. We always bring an impartial and critical perspective to bear on our work.

The DPA takes account of the interests of all parties concerned, but adopts an independent and considered approach when determining and formulating its standpoints and priorities. Our independence also comes to the fore in the way we form our opinions: we conduct investigations in an objective, critical and impartial manner.

Openness

The Data Protection Authority maintains close ties with other actors in its field. We are accessible to people and organisations wishing to pass on or obtain information about rules and risks. We are transparent where possible. We communicate actively about our work processes and our decisions, stimulate public debate and explain the rules. Our accessible use of language and transparency about what we do make us more effective and increase our legitimacy.

What we mean by openness is that we have made a conscious decision to maintain an active public profile, stay in touch with our supervisory domain, and ensure we are accessible to all people and organisations. We take specific account of the fact that not all people are equally able to deal with organisations on their own. We aim to be a helpful conversation partner to organisations seeking to implement a high level of data protection. We are keen to help businesses and public authorities generate ideas for developing products and services in a privacy-friendly manner. We are also transparent about the work we do, our objectives and our resources, and we are accountable for our results. We communicate about breaches identified but also make a point of communicating – proactively – in situations where the protection of personal data is safeguarded effectively.

Expertise

The Data Protection Authority's staff are experts in their field and develop continuously in line with the changing context. The DPA encourages the development of individual staff members and works to improve the organisation as a whole with a view to being a modern supervisory authority.

The DPA attaches great value to having in-house expertise. It is the product of our efforts to ensure that staff have the required specialist knowledge, work professionally and demonstrate commitment. We see professional development as an ongoing requirement for all people within our organisation. We invest in staff training. In this regard we seek to work with other supervisory authorities, government bodies and universities. Expertise also means that our staff are familiar with the issues that matter. On the basis of its thorough knowledge of a theme or field of supervision, the DPA determines its position proactively and selects the tools that are most effective within that theme or field.

Effectiveness

Because we have to deal with national and international developments, our responses are carefully considered. We choose the approach that will be most effective in the specific situation. We operate decisively but always keep our focus on people's fundamental right to protection.

The DPA's supervisory domain is broad and with the entry into force of the GDPR the DPA is gaining a number of sizeable tasks. This means that we have to prioritise, intervene intelligently, and use our capacity as effectively and efficiently as possible. To achieve these aims, we seek to work together with various industry bodies and other stakeholders. We focus in particular on data protection officers. Data protection officers can be seen as the internal supervisors within organisations; they monitor the application of and compliance with the GDPR.

Effective supervision demands decisive action. To operate effectively, the DPA employs a range of supervisory and enforcement instruments. These instruments include actions such as sending a warning letter, holding a remedial meeting to address a breach of a standard, launching an investigation, and imposing a penalty payment or a fine. Our guiding principle is to choose the enforcement instrument that is the least severe and the most effective. To operate effectively we need more than just a successful intervention policy. We must also use our expertise to inform, advise and communicate. In other words, we offer guidance where possible, but take action where necessary.

2. Supervision 2018-2019

2.1 Promoting compliance

The principal goal of our supervision is to promote compliance with privacy legislation. Prior to the entry into force of the GDPR, the DPA made a priority of raising awareness among the general public, businesses and public authorities of the changes this legislation would bring. We conducted an information campaign, gave presentations and held workshops. We made it easier for people to contact us by phone and made practical tools available enabling businesses and other organisations to make their operations 'GDPR compliant'.

Offering guidance

In the year ahead the DPA will continue to promote compliance with privacy legislation, in part by offering guidance to individuals and organisations in the form of information and advice. We also support organisations by offering practical tools, providing clear explanations of standards and promoting the establishment of standards that are recognised across Europe. In addition, we assess requests for prior consultations and licence applications for processing data relating to criminal convictions and offences, and we promote the creation of codes of conduct, among other things. We also invest in establishing and maintaining good relations with data protection officers. We ensure they can get in touch with us easily, and we keep them informed and answer any questions they may have.

Handling complaints

The GDPR has introduced greater scope for submitting complaints. The DPA handles complaints that indicate a possible breach of the rules on processing personal data. The phone lines of the Privacy Information and Reporting Point are open five days a week for people wishing to ask questions, pass on

information or submit a complaint. In handling complaints the DPA aims to empower people to exercise their rights. We help them by offering tools and providing support and guidance where necessary. If the rules have been breached, we respond by taking action if necessary. By handling complaints we help to promote compliance with the law.

Advising on legislation

In its role as legislative adviser, the DPA helps to ensure that legislation is compatible with the Charter of Fundamental Rights of the European Union, the Treaty on the Functioning of the European Union (TFEU) and the GDPR. We assess, for example, whether any infringement of the right to protection of personal data is justified and whether it is proportionate in light of the legislation's objective. To this end we draw on the knowledge and experience we have gained from our work in our supervisory domain and the exercise of our supervisory and enforcement powers. The DPA provides both solicited and unsolicited advice and consults with the legislature. We actively contribute ideas on current questions concerning the use of personal data with a view to promoting fair and lawful service provision by public authorities.

2.2 Monitoring compliance

Besides offering guidance and handling complaints in order to promote compliance, it is also important to actively monitor compliance. Businesses and public authorities must be able to demonstrate that they are acting in accordance with the GDPR.

The accountability required by the GDPR compels organisations to demonstrate compliance with the GDPR. The fulfilment by an organisation of its accountability obligations does not necessarily signify full compliance with the GDPR. However, it is a good indication of the degree to which the organisation is taking implementation of the GDPR seriously and has given thought to the GDPR's main elements (including the basis for processing data, purpose limitation and security).

To determine whether the accountability requirements under the GDPR are being fulfilled, we monitor compliance with one of these requirements in various sectors. We do so in the expectation that information about the outcomes of our monitoring will increase the learning capacity of organisations with regard to compliance with the GDPR. We therefore intend to communicate actively about our monitoring activities and our findings.

2.3 Risk-based supervision

In keeping with the GDPR, the DPA puts the public first. Data is increasingly being processed out of people's sight. The DPA adopts a risk-based approach to supervision, paying particular attention to possible breaches of personal data protection that could affect large numbers of people. Over the coming period we will focus in particular on public authorities, healthcare institutions and businesses that trade in personal data. We will also take action in other sectors, for example in response to new developments and complaints.

Public authorities

Central and local government, implementing organisations, the police and the criminal justice authorities possess a large quantity of personal data, much of which is of a sensitive nature. People are often obliged to give their personal data, so they must be able to rely on the public authorities abiding by the rules when they process that data.

The DPA places special emphasis on how personal data is secured, and whether the processing of personal data is founded on a legitimate basis, especially when data is being exchanged. We also check compliance with the obligation to maintain records of processing activities, the obligation to appoint a data protection officer, and how the data protection officer is positioned within the organisation and enabled to discharge the tasks and duties conferred upon him or her by the GDPR.

Healthcare

Besides public authorities, healthcare institutions also hold large volumes of personal data, in particular medical data. Because of its sensitive nature, data about someone's health is a special category of personal data. The GDPR, like the former Personal Data Protection Act, sets stricter requirements for the processing of sensitive personal data of this kind. Good security is important in order to prevent patients' medical data falling into the hands of unauthorised persons. In accordance with the principle of doctor-patient confidentiality patients must be able to rely on their medical data remaining a matter for them and their doctor(s) alone.

For healthcare institutions, as for other organisations, the DPA places special emphasis on how personal data is secured and whether the processing of personal data is founded on a legitimate basis, especially when data is being exchanged. Here too the DPA monitors compliance with the obligation to maintain records of processing activities, the obligation to appoint a data protection officer, and how the data protection officer is positioned within the organisation and enabled to discharge the tasks and duties conferred upon him or her by the GDPR.

The trade in personal data

The trade in personal data has increased in recent years. Data brokers collect vast quantities of consumers' personal data via a large number of online and offline sources. They use it to create profiles which they pass on or sell to other data brokers and/or customers who use it to make decisions about people's creditworthiness, for example, or for direct marketing purposes. The best-known data brokers are credit agencies, but there are many more businesses and organisations that trade in personal data (which they often hold for a different purpose).

People are often unaware of the quantity of data involved or what personal data is exchanged, with whom, and to what end. What is more, people are generally unfamiliar with the phenomenon of profiling. People who are not aware that their data is being processed and their profiles passed on to other parties face a substantial risk. They may find out only after a decision has been taken which affects them, such as the refusal of a loan or a subscription. Another risk lies in the fact that data and profiles may contain errors. and this could have far-reaching consequences for the people concerned. As a consequence, people lose control over their data.

Over the coming period the DPA will focus on the trade in personal data with the primary aim of ensuring that businesses and organisations that sell personal data only do so on a legitimate basis and comply with the information requirements laid down by the GDPR.

Data breaches

The processing of large volumes of sensitive data increases the risk and consequences of data breaches. Effective security is therefore essential. Since mandatory data breach notification was introduced on 1 January 2016, the DPA has focused on encouraging controllers to report data breaches. In 2016, the DPA

received nearly 6,000 reports of data breaches. In 2017 more than 10,000 breaches were reported, a rise of over 70%. In a number of cases security was deficient or, at best, inadequate. Inadequate security entails considerable risks for the protection of personal data, especially if it results in a breach involving sensitive personal data such as medical data or data about political preferences or sexual orientation, . But there is also a risk if the breach involves people's names, addresses, credit card details, email addresses, or even their citizen service number (BSN).

The GDPR lays down a number of new requirements as regards the duty to report data breaches. For example, organisations must now document all data breaches, and not just those they have reported. They must keep a register of data breaches. In addition, the penalties that may be imposed were increased when the GDPR was introduced.

In 2018-2019 the DPA will devote extra attention to unreported data breaches and data breaches caused by or related to serious shortcomings in security.