Whitepaper: Data Protection: Compliance is a Top-Level Sport

Edition 201705

About the author

Renate Verheijen
Secura (formerly known as Madison Gurkha)

Content

Data Protection: Compliance is a Top-Level Sport

1 Introduction

In this article, Renate Verheijen, Legal & HR Counsel at Madison Gurkha, maps out the consequences of the General Data Protection Regulation (GDPR) and guides you through the challenges that lie ahead. Find out how you are doing and what steps you need to take to become or remain compliant.

Data processors have been given until May 25, 2018—regardless of whether they are based inside or outside the EU—to switch to a data processing method that complies with all the requirements and standards set out in the General Data Protection Regulation (GDPR)[1]. Since we tend to be rather enthusiastic about gathering personal data for general or commercial objectives, the European Union has set itself the task of creating a forceful, coherent framework for data protection and ensuring that the only personal data processed is the data required for the purpose for which it is used. Given the content, scope and number of provisions, it appears that the outcome is more comprehensive than just a framework. It concerns a reasonably strict set of obligations that need to be observed by anyone processing personal data.

2 Application of the GDPR

Before rolling up your sleeves and getting stuck in, it is worth examining what falls within the scope of personal data and the processing personal data, and whether the regulation also applies to the data to be processed by you. In Art. 4, clause 1 GDPR, personal data is defined as any information relating to an identified or identifiable person. A person is considered identifiable if the person can be directly or indirectly identified. This is already the case when an identifier is used, such as a name, identification number (for example, a customer number, payroll number, membership number or account number or name), a person's location data, an online identifier (for example, an IP address, email address, GPS coordinates of a mobile device), or if one or more facts are gathered that are characteristic of the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person. In fact, it doesn't take much at all for data to be considered personal data. In cases when you would probably assume that data is not identifiable, because the information is not directly visible or is stored across a number of different places, or because you have taken steps to anonymize the personal data, the opposite may be true. Unintended or deliberate combinations of these items of non-identifiable data, or the different places where the data is stored becoming linked may cause the data to become identifiable, even if you have taken no action to cause this. Leaving aside making your data anonymous, it is important that you take all possible steps to prevent your data becoming identifiable. Non-identifiability or anonymity alone provide insufficient guarantee if you process the data.

[1] Regulation (EU) 2016/679 of the European Parliament of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation: referred to below as GDPR), OJ L 119 of May 4, 2016, p. 2, clause 7.

The rules and obligations of the GDPR apply as soon as you start processing data. Processing is defined as performing an action or set of actions, automated or otherwise, such as collecting, recording, sorting, structuring, editing or amending, using, retrieving, accessing, issuing data by sending, circulating or making data available in another way, aligning or combining, protecting, deleting or destroying data (Art. 4, clause 2 GDPR). Whenever you process personal data, other than as a purely private action, the GDPR is applicable. Exceptions are made for processing that falls outside the scope of European Union legislation or when personal data is processed by competent authorities in order to prevent, investigate, detect or prosecute criminal activities. Furthermore, the regulation does not apply in the event that a person has died, and other rules apply in this case[2].

3 Principles

Now that it is clear when the regulation is applicable, it is time to face the challenges ahead. Whereas the Dutch Personal Data Protection Act (Wbp) refers to a few rights of the natural persons whose data is processed,[3] the GDPR assigns more weight to those rights and refers to 'Principles relating to processing of personal data' (Art. 5, clause 1 GDPR). You must demonstrably implement these principles and observe them. What are the principles concerned?

1. The principles of lawfulness, fairness and transparency

The personal data must be processed in a manner that is lawful in relation to the data subject, with that person's consent (Art. 7, 8 GDPR). Strict rules apply to processing special personal data[4] (Art 9 GDPR).

2. The principle of purpose limitation

Personal data can only be processed based on explicitly described and justified objectives and must not be used for other objectives (Art. 5, clause 1, sub b GDPR).

3. The principle of data minimization

The information must be relevant for its purpose, processing and collecting data must be limited to what is necessary for the objectives (Art. 5, clause 1, sub c GDPR).

4. The principle of trueness, accuracy

Reasonable measures must be taken to rectify or remove any

[2] Clause 27 GDPR, p. 5. Given the subject of this article and the limited length, there is no space to elaborate on this.

[3] 3 These rights are set out in Art. 35–42 Dutch Personal Data Protection Act (Wbp) and include the right to amend, correct, supplement, protect or delete the data; the right to object to personal data being used; the right to information concerning data processing and the right not to be subjected to decision-making based on 'profiling' (this is about a decision solely made on the basis of the automated processing of personal data destined to gain an image of certain personal characteristics of the data subject, where the decision has legal or significant consequences for the data subject).

[4] The data concerned is data relating to race or ethnic origin, political beliefs, religious or philosophical convictions political beliefs, membership of a trade union, processing of genetic details, biometric data with a view to identifying a person, data concerning health, sexual conduct or sexual orientation.

inaccuracy with a view to the objectives used (Art. 5, clause 1, sub d GDPR).

5. The principle of storage limitation

The data must be stored in a format that makes it possible to make the data subjects non-identifiable as soon as the objective of the data processing has been achieved. Exceptions are storage in the general interest, storage in the interest of scientific, historic or statistical study (Art. 5, clause 2, sub e GDPR).

6. The principle of integrity and confidentiality

You must take appropriate technical and organizational measures to guarantee suitable protection for processing the personal data. (Art. 5, clause 1, sub f GDPR). If these principles are breached, the Dutch Data Protection Authority[5] can impose an administrative fine, after considering all circumstances and interests involved, of up to a maximum of EUR 20 million or, if your global annual turnover is higher, of 4% of it (Art. 83, clause 5, sub a GDPR). In the event that the rights of the data subjects are breached under the Dutch Personal Data Protection Act (Wbp), the maximum fine for 2016 is EUR 820,000, which immediately highlights the weight assigned to the principles, resulting in severe sanctions imposed when they are breached. However, not every breach automatically leads to a fine. If it appears that you made the necessary efforts and that a breach was in no way caused by your actions, or that you are demonstrably adhering to the instructions given by the supervisory body, no further action will be taken.

4 The Rights of Data Subjects

Furthermore, the number of rights assigned to data subjects has been extended under the GDPR. The rights of data subjects that you must respect and observe can be found under Articles 12 to 22 GDPR.

These include:

1. The right of the data subject to be informed when personal data relating to them is gathered;
2. The right of the data subject to other information when the data has not been obtained from the data subject;
3. The data subject's right of inspection; the right to correct and delete data (the right to be forgotten);
4. The right to processing restrictions;
5. The duty to be informed of corrections to the personal data or to processing restrictions;
6. The data subject's right to have his data transferred to other data processors;
7. The right to object and the data subject's right not to be subjected to automated individual decisionmaking,including profiling.

Any breach of these rights—arising from the above principles—qualifies for the same sanctions and is therefore no less important, in terms of compliance, than the principles. It is therefore essential to set up procedures in advance for complying with these principles and rights. You must be able to demonstrate these procedures and communicate them to the data subjects. There is still work to be done, so roll up those sleeves a little higher still! Another set of obligations awaits. These vary depending on the role you play in processing personal data.

[5] This will be, or rather, it continues to be the supervisory authority under the GDPR.

5 Your Obligations as Controller[6]

Central to the obligations when processing personal data is that the required level of data protection must already be taken into account at the design stage for the processing method (Privacy by design). The GDPR is fairly brief on the obligations to be met by referring to a general starting principle that, taking into account the available technology, implementation costs, scope, context and objective of the data processing and the possible gravity of the risks for the data subjects, appropriate technical and organizational measures must be taken to observe the data protection principles during data processing, compliance and protection of the rights of the data subjects (Art. 25 GDPR).

As guidance for arranging these measures, you can continue to use the 2013 Dutch Data Protection Authority's Guidelines for personal data protection (Richtsnoer Beveiliging van persoonsgegevens[7]).

These guidelines were written in association with the then draft Regulation of the European Commission, which has now become definitive. These guidelines were written in association with the then draft Regulation of the European Commission, which has now become definitive. These two documents are closely aligned. For example, you can take appropriate measures based on a risk analysis that will enable you to guarantee a suitable protection level for processing personal data. The risk analysis is known as the Privacy Impact Assessment (PIA), and is also referred to as a data protection assessment (Art. 35 GDPR). Under the Dutch Personal Data Protection Act (Wbp), the assessment fell outside the scope of Art. 13 Wbp and had no formal status. It does now. In the event of large-scale personal data processing, the assessment is compulsory, as well as for the large-scale monitoring of publicly accessible areas, or the systematic and extensive evaluation of personal aspects relating to a natural person, based on automated data processing, such as profiling. In addition, the Dutch Data Protection Authority can draw up a public list of types of data protection for which it does or does not make a data processing impact assessment compulsory. It is therefore important for you to keep closely following any new developments of the Authority. Aside from that, the risk analysis will help you gain an insight into what you need to do.

The data protection impact assessment was developed by NOREA (the professional association of IT auditors in the Netherlands) in collaboration with the Dutch Data Protection Authority, the Dutch national audit service (Auditdienst Rijk), PWC—naturally not entirely devoid of interest—and PBLQ/HEC[8].

You must complete a questionnaire, assess its impact with the use of a guide and take any additional measures before producing a report and submitting it to an independent auditor for evaluation. Not surprisingly, the move is welcomed by PWC. If it follows from there that the data processing you have in mind involves a high risk, you will have your work cut out, to put it mildly. In that case, in conformity with Art. 36 GDPR, you will need to apply to the Dutch Data Protection Authority for a prior consultation. It is a fairly time-consuming and laborious procedure as part of

[6] Art. 4, clause 8 GDPR describes a controller as "a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means for the processing of personal data." Where "the purposes and means of such processing are determined by Union Law or Member State Law, the controller or the specific criteria for its nomination may beprovided for by Union law or by Member State law."

[7] https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_beveiliging_van_persoonsgegevens.pdf

[8] Privacy Impact Assessment (PIA), "Introductie, handreiking en vragenlijst" (introduction, guide and questionnaire), version 1.2, November 2015, NOREA (the professional association of IT auditors in the Netherlands). https://www.norea.nl/download/?id=522

which you have to submit all information and await the written advice of the Authority. You are naturally obliged to follow the advice.

If special personal data is processed, it is necessary to take account of the necessary security level at the design phase (Security by design). For that reason, you need to use Privacy Enhancing Technologies (PET): the required protection level will be the guiding principle for choosing security measures.

The next step is to design or to update suitable organizational and technical measures, using the tips and tricks from your auditor in a neat report, in order to protect the processing.

You do this by establishing the reliability requirements.

What matters here is the extent to which the information provision organization can rely on an information system. Four protection factors play a role:

1. Availability

Measures that guarantee that users can access the data and related corporate resources at the right times.

2. Integrity

Guaranteeing that the data and data processing are accurate, up to date and complete.

3. Confidentiality

Guaranteeing that information is only accessible to those authorized to access it.

4. Verifiable

Guaranteeing that it is possible to verify with sufficient certainty whether the above three factors are met.

Based on a "plan-do-check-act" cycle, you can design these measures step by step, before updating, checking, evaluating and adjusting them. All these factors are contained in Art. 32 GDPR. Before you produce these protection measures, I recommend that you consult the Dutch Data Protection Authority's Guidelines for personal data protection and that you follow the approach prescribed. The guidelines frequently refer to standard NEN-ISO-IEC 27002:2007 (which has since been updated and I recommend that you consult the latest version), which will bring you in line with the GDPR.

After all, the GDPR boosts compliance with the certification requirements. The GDPR does not go as far as explicitly referring to the NEN-ISO guidelines (due to the diversity in certifications for the member states and the sector-specific adjustments that involve variations in the standards) but explicitly indicates that certification mechanisms can offer significant support to demonstrate that you comply with the relevant guidelines as controller[9]. Approved codes of conduct can also contribute to this. For example, small and medium-sized enterprises can produce sector-specific codes of conduct and submit them for approval to the Dutch Data Protection Authority, and they can adjust the implementation of the GDPR to the circumstances and scope of the personal data processing[10]. Furthermore, the Data Protection Authority can approve binding corporate rules for a group of undertakings or enterprises in relation to personal data processing, and the way data is

[9] Articles 24, 25, 32, 42, 43 GDPR.
[10] Articles 24, 32, 40, 41 GDPR.

transferred between the members of the group (potentially located in different member states) (Art. 47 GDPR).

What is new is that you, as controller, are obliged pursuant to Art. 30 GDPR to keep a record of the following data:

1. The name and contact details of you as controller and of the data processing officer appointed by you and the processor, if applicable;
2. The processing objectives;
3. A description of the categories of personal data;
4. The categories of recipients to whom personal data has been or will be supplied, including when these are international organizations or located in third countries;
5. The third country or international organization to which you transferred personal data and the documents concerning appropriate safeguards for governance;
6. The envisaged periods of time within which the different categories of personal data must be deleted;
7. A general description of the technical and organizational security measures.

In conformity with the Dutch Data Leaks (Reporting Obligation) Act (Wmd), the GDPR also stipulates that you, as controller, are obliged to report a data leak to the Dutch Data Protection Authority within 72 hours of becoming aware of it (Art. 33, clause 1 GDPR). The GDPR also stipulates what the notification must include (Art. 33, clause 3, sub a–d GDPR) and under what circumstances you must inform the data subjects regarding the data leak and what must be included in the communication (Art. 34, clause 1 and clause 3 sub a–c GDPR).

6 Your Obligations as Processor[11]

The GDPR indicates quite firmly that the controller can only engage you as a processor if you can offer suitable guarantees regarding your implementation of appropriate organizational and technical measures, which means that all requirements in the regulation are met and the privacy of the data subjects is protected. You work exclusively on instructions from the controller unless there is an obligation to process arising from Union or Member State law (Art. 29 GDPR). You as processor can only subcontract the processing with the controller's written permission (Art. 28, clause 3 GDPR).

If the sub-processor defaults on its compliance, you remain fully liable as processor in relation to the controller (Art. 28, clause 4 GDPR). All your obligations as processor towards the controller are recorded in a processing contract. Contrary to the Dutch Personal Data Protection Act (Wbp), the GDPR stipulates what needs to be included in the processing contract (Art. 28, clause 3, sub a–h GDPR). In addition, you must assist the controller with the obligations he is under as set out in Articles 32–36 GDPR. The controller is entitled to perform an audit to check whether you meet the protection provisions, to verify your internal procedures and whether you have implemented appropriate measures and safeguards.

Like the controller, you are obliged to keep a record of all categories of processing activities that you carry out on behalf of your controller (Art. 30, clause 2, sub a–d GDPR). It concerns the following data:

1. Your name and contact details as processor and any subcontractors you may have engaged, as well as the controllers on whose behalf you process data and the contact details of a data protection officer appointed by you and the controller, if applicable;
2. The categories of processing carried out on behalf of all the controllers you work for;

[11] Art. 4, clause 8 GDPR describes the processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3. The transfers of personal data to a third country or an international organization, including the countries or organizations concerned, and the documentation of appropriate safeguards;
4. A general description of the technical and organizational security measures.

The Dutch Data Protection Authority can ask to be sent this record, as well as the record kept by the controller (Art. 30, clause 4, GDPR). If you fail to meet your obligations as controller or as processor, the GDPR's fining policy in relation to the principles of data processing and the data subjects' rights is slightly milder. The fine imposed in the event that you breach your obligations will be up to EUR 10 million. If your company has a higher annual turnover, the maximum fine will be 2% of the global annual turnover (Art. 83, clause 4, sub a–c GDPR). Fines are naturally not imposed for no reason, but after careful consideration of all interests concerned, taking into account the circumstances.

7 The data protection officer (Articles 37-39 GDPR)

Whereas the Dutch Personal Data Protection Act (Wbp) (Articles 62 and 63 Wbp) provides an option to appoint an officer who can support, advise on and monitor implementation and security for personal data processing, the GDPR is more explicit about this officer. The officer must have an independent status to monitor your organization's compliance with the GDPR, in a supportive and advisory role. You are not allowed to give this officer instructions, but you can pay him to act independently. If you are considering appointing an existing member of staff who can combine this role with his current role, then bear in mind that the GDPR specifies clearly that there must be no conflict of interest. You may also be hoping to come off lightly by using the 'Social Return' job creation scheme, but the GDPR has specified such rigorous demands on knowledge and skills that this would not work and you are facing an expensive addition to the payroll.

The ideal candidate can be described as a cross between an IT security expert and a shrewd lawyer specialized in IT and personal data. This is an extremely rare combination, which means that you will need to conjure up someone with the help of a solid, healthy training budget. You will therefore understand my admiration for the data officers already holding the role. Given the fact that it is an independent position, you will not be able to dismiss this person based on their performance.

Fortunately, you are not necessarily obliged to appoint such an officer[12]. If you do decide to appoint someone to the role, without an obligation to do so, you will nevertheless need to adhere to all provisions in the GDPR in relation to that position. The proverb 'Look before you leap' is therefore appropriate in the circumstances.

8 Conclusion

It is relatively safe to conclude that there are plenty of challenges ahead. You will not be the only one feeling hot under the collar when listing all these action points on your to-do list. The time, energy and money that you undoubtedly planned to spend elsewhere, will now be partly absorbed by these implementation requirements. Needless to say, you will have to cover the costs, and, no,

[12] Three sets of circumstances have been set out in which appointing a data processing officer is compulsory: Art. 37, clause 1 GDPR contains a list.

your customers do not expect you to pass these costs on to them. With the GDPR, you may wish to swap your business suit for a professional sports kit. Compliance has been turned into a top-level sport, with sympathetic professional personal auditors and a coach (the data processing officer) guiding you to the finishing line. Anyone who fails to reach the finish (or in time) will be subjected to a punishing exercise regime and if the results fall short, your organization will foot the bill.

I can only advise you to draw up a sound strategic plan and to produce a proper inventory in advance of the tasks to be completed and the time needed to implement the plan. Develop in-house connections with the people who can provide you with partial assistance, and don't forget your customers. Produce a realistic and pragmatic project plan.

Systematically follow the GDPR as well as a 'plan-do-check-act' cycle for the data protection impact assessment. If you then take suitable measures, complying with both the Dutch Data Protection Authority's Guidelines and the current NEN-ISO-IEC 27002 standard, you are well on your way to becoming a top-level athlete. Operating at that level requires investment, discipline and perseverance. Unfortunately, no prizes are up for grabs.

9 About EXIN and Secura

EXIN is the global independent certification institute for professionals in the ICT domain. With more than 30 years of experience in certifying the competences of over 2 million ICT professionals, EXIN is the leading and trusted authority in the ICT market. With over 1000 accredited partners EXIN facilitates exams and e-competence assessments in more than 165 countries and 20 languages. EXIN is co-initiator of the e-Competence Framework, which was set up to provide unambiguous ICT certification measurement principles within Europe and beyond.
www.exin.com

Madison Gurkha was established in 2000 and is an independent specialist in (technical) IT security. It is our mission to help our clients improve their IT security posture by delivering world-class, independent security advice, test and assessment services. In order to achieve our mission we offer a service portfolio that consists of three divisions: 'Advisory & Audit', 'Security Assessment' and 'Training & Awareness'. In October 2017, Madison Gurkha changed their name to Secura: Your trusted IT security partner.
https://www.secura.com/

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER