LOYENS & LOEFF

2018

EDITION 118

Quoted

Privacy compliance has truly become a boardroom topic: what do you really need to know in order to be able to take part in the conversation?

LOYENS & LOEFF

In this edition

Privacy compliance has truly become a boardroom topic: what do you really need to know in order to be able to take part in the conversation?

You will most likely be aware of the fact that the European privacy legislation will enter into force on 25 May 2018: the General Data Protection Regulation (**GDPR**).[1] Every organisation that processes personal data – which is the vast majority of organisations in the Netherlands – will be affected by this legislation. It is therefore important to know what will actually change under the GDPR and to determine the impact thereof on your organisation. This edition of Quoted will provide you with the necessary information in order to enable you to ask the right questions within your organisation, and to check whether your organisation is prepared for the GDPR.

What is the GDPR?

The GDPR is a European Regulation which will enter into force on 25 May 2018 throughout the European Union (**EU**), whereby it will largely harmonise privacy and data protection legislation throughout the EU.

The GDPR will be directly applicable in all EU Member States, but Member States will have the option to derogate from the GDPR in their own national legislation on certain points. In the Netherlands, the national derogations have been established in the Implementation Act of the General Data Protection Regulation (*Uitvoeringswet Algemene Verordening Gegevensbescherming,* **Implementation Act**).[2] As a result, differences may exist within the EU between various national implementation acts, which may lead to a difference in the applicable laws. For instance, with regard to the processing of special categories of personal data, such as personal data related to health, race or ethnic origin. These differences in national implementation legislation may be relevant for your organisation if it has group companies in different EU Member States.

Does my organisation have to comply with the GDPR?

The GDPR applies to the *processing* of *personal data*.

Personal data are data based upon which a living individual can be identified (directly or indirectly), such as contact details, a photo, a CV, a (business) email address, a social security number, medical data, but also an IP address, identification cookies, location data or information about a person's income may qualify as personal data. In addition, there is the category of special or sensitive personal data. This type of personal data is given extra protection and includes information about a person's health, religion or a criminal record.

Data that are not considered personal data are data of legal entities, deceased persons or anonymised personal data.[3] Despite the fact that data of a legal entity itself are not personal data, data of persons who work for a legal entity do qualify as personal data. For example, the business email address or direct business phone number of an employee does qualify as that employee's personal data.

Please note: when assessing whether certain information qualifies as personal data, the context is very important. It is possible that certain information does not qualify as personal data in itself, but in combination with other data, it does qualify as personal data.

What qualifies as the processing of personal data?

Processing includes almost every action that can be performed with personal data. This includes viewing, collecting, storing, forwarding, destroying, recording, retrieving, shielding, organising, making available and updating data.

As is also the case under the Dutch Data Protection Act (*Wet bescherming persoonsgegevens,* **Wbp**), the GDPR makes a distinction between the role of the controller[4] and

1 Regulation (EU) 2016/679. N.B. where reference is made in this Article to the GDPR, this should include the applicable national implementing acts.

2 The legislative proposal for the Implementing Act for the General Data Protection Regulation was submitted to the House of Representatives on 13 December 2017. The envisaged date of entry into force is 25 May 2018.

3 The threshold in order to qualify as anonymised personal data is relatively high. In the case of anonymised data, it is not possible to identify the data subject. Anonymisation must be irreversible. If a 'key' is still available to identify the person concerned, it does not qualify as anonymised data, but as pseudonymised data. The GDPR does apply to pseudonymised data.

4 In the Wbp, a '*verwerkingsverantwoordelijke*' (controller) is referred to as a '*verantwoordelijke*' (controller).

that of the processor[5]. In short, the controller is the entity that determines the purpose and means of the processing of personal data, while the processor is the entity that processes personal data on behalf of the controller.

What will actually change?

An important change is that the GDPR emphasises upon the accountability of organisations – also referred to as the accountability principle. Organisations must be able to demonstrate that they comply with the GDPR. In this context, it is important to, amongst other things, maintain i) a formal, written, internal record of processing activities[6], ii) an internal policy on how staff should handle personal data, iii) an internal policy on how to act in the event of a data breach, and iv) a policy concerning retention periods.

Another important change is that under the Wbp, the obligations are mainly imposed on the controller. The GDPR however also imposes more direct obligations on the processor, such as the obligation to take adequate security measures and to maintain a record of processing activities.

The GDPR strengthens the rights of persons whose personal data are processed (also referred to as data subjects) and introduces a number of new rights. These include the right of a data subject to request an organisation to delete the personal data pertaining to them in certain cases (the right to be forgotten) and the right to receive their personal data in a structured, frequently used and machine-readable format so that these data can be easily transferred to another organisation (the right to data portability). It is likely that adjustments to the business operations of your organisation are required in order to be able to meet these strengthened and new rights of data subjects in a timely manner.

In addition, the GDPR contains an extensive information and transparency obligation for organisations. This means that data subjects must be thoroughly informed about the processing of their personal data. You may already have a privacy statement on your website. Nevertheless, since the GDPR is extending the obligation to provide information compared to the current legislation, your privacy statement will probably have to be amended. For instance, the GDPR also requires organisations to inform data subjects of the legal basis on which their processing activities are based, as well as on the applicable retention periods.

Compared to current legislation, the GDPR has a broader scope of application. Non-EU based organisations processing personal data may also be covered by the GDPR (for example, a web shop based in the U.S. that offers products to individuals in the EU). In such cases, it is likely that a designated representative will have to be assigned in the EU. This representative can be approached in addition to, or instead of, the organisation concerned by both the regulators as well as the data subjects.

In certain cases, the GDPR also contains the obligation to appoint a Data Protection Officer (**DPO**) with the task to supervise the application of – and compliance with – the GDPR within an organisation. A DPO is mandatory for (i) government bodies and public organisations, (ii) organisations that regularly and systematically monitor data subjects on a large scale as part of their core activities, e.g. camera surveillance or profiling of persons for the purpose of making risk assessments, and (iii) organisations that process special personal data on a large scale, e.g. hospitals. This obligation is new. Under the current Dutch regime, a DPO is not mandatory.

In addition, the GDPR introduces the 'one-stop shop' rule. This means that organisations that process data in several EU Member States for the purpose of certain cross-border processing operations will, in principle, only have to deal with one privacy supervisor: the 'leading supervisor'. This is the supervisory authority of the principal or only place of business, of the controller or the processor.

What will not change?

As stated above, the GDPR will introduce new obligations for organisations, but it is a misunderstanding that the GDPR will change all regulations with regard to the protection of personal data.

Privacy legislation is after all not entirely new. The current privacy legislation, laid down in the Wbp, is based on a

5 In the Wbp, a '***verwerker***' (processor) is referred to as a '***bewerker***' (processor).

6 A record of processing activities should describe, among other things, which personal data and which categories of personal data are processed, for which purposes the data are processed and to which parties the data are transferred. Article 30 of the GDPR contains a complete overview of the requirements to be met by a record of processing activities. Article 30(5) of the GDPR makes an exception to the obligation to keep a record of processing activities for certain organisations. In practice, this exception cannot be invoked in many cases.

European directive.[7] The GDPR builds on the existing obligations under that directive. Many concepts with regard to the protection of personal data are therefore already known and mandatory under the current privacy legislation.

Another common misunderstanding is: 'those who process personal data must from now on always first request the consent of the data subjects'. This is incorrect. Consent, as under the current legal regime, is only one of the six possible legal grounds on which a data processing operation can be based. The GDPR does however contain stricter requirements for obtaining valid consent. In addition, data subjects should always have the opportunity to withdraw their consent just as easily as they gave their consent. In practice, this means that organisations should generally, and where possible, base their processing activities on a different legal basis than consent.[8]

The legal grounds on which processing of personal data can be based will not change under the GDPR. Nevertheless, this is a good time to check within your organisation whether there is a legal basis for all the processing activities that take place.

Another misunderstanding is the idea that personal data may no longer be transferred to countries outside the EU. The GDPR sets specific requirements for the transfer of personal data outside the EU. This is important, for example, when personal data of a Dutch company are stored on a server in the United States, which is controlled by an American company or parent company. It is important that the necessary measures are in place for such a transfer of personal data. One of these measures is, for example, agreeing with the US company on standard data protection clauses approved by the European Commission for the transfer of personal data.[9] However, also this requirement is already applicable under current legislation, so action is only required if it has not yet been properly arranged within your organisation.

Why is everyone talking about the new privacy legislation?

One of the objectives of the GDPR is to strengthen the enforcement possibilities of national supervisory authorities. To this end, the GDPR introduces high fines of up to €20 million or, if higher, 4% of global annual turnover. This highest maximum category of fines applies, for example, to violations of provisions relating to the rights of data subjects or relating to the failure to comply with an order issued by a supervisory authority.

For other infringements, such as infringements of security obligations under the GDPR, the maximum fine is lower, namely €10 million or, if higher, 2% of the global annual turnover. In any case, the fines that can be imposed are substantial and give rise to a great deal of controversy.

Will the high fines actually be imposed?

The question that is of concern to many is whether the Data Protection Authority (*Autoriteit Persoonsgegevens,* **AP**)), will actually impose fines of this magnitude as from 25 May 2018. Although the AP has announced that it will maintain a strict enforcement policy, it has not yet published a policy on this matter.[10] A few refinements will be made below to the 'fear' of high fines.

Firstly, it should be borne in mind that such amounts are ceilings for fines. This does not, of course, alter the fact that the AP is authorised to impose the maximum amount of the fine. The GDPR does not mention any concrete ranges within which fines for certain infringements may fall. In addition to the principle that fines must be effective, proportionate and dissuasive, the GDPR stipulates that the imposition of a fine must take account of all the circumstances of the case. The GDPR also mentions a number of circumstances that must be taken into account in determining the amount of the fine, such as the nature, seriousness and duration of the infringement, the number of data subjects involved, the extent of the damage, the intentional or negligent nature of the infringement and any previous relevant infringements.

7 Directive 95/46/EC of the European Parliament and of the Council of the European Union adopted on 23 November 1995 on the protection of individuals with regard to the processing of personal data.

8 Article 6 of the GDPR lays down the legal grounds for the processing of personal data.

9 These are standard contracts drawn up by the European Commission which – unchanged – provide a valid basis for transferring personal data to a country outside the EU that does not provide an adequate level of protection.

10 https://fd.nl/economie-politiek/1204827/miljoenenboete-facebook-is-kinderspel-bij-wat-komen-gaat.

The imposition of fines is not the only mean of enforcement available to the AP. The AP can also take corrective measures, such as a reprimand, the imposition of a temporary processing restriction or a processing prohibition. The AP can also issue a warning prior to the imposition of a fine or other corrective measures. In addition, the AP is authorised in certain cases to impose an order subject to a penalty for non-compliance or an administrative enforcement order. These are remedial sanctions with which the AP can oblige organisations to take measures within a certain period of time, subject to a penalty or an administrative enforcement, as the case may be.[11] The legislator has explicitly indicated in the explanatory notes to the Implementing Act that these are in practice effective means of ending infringements of rules relating to the protection of personal data.[12]

It is striking that the so called "Article 29 Working Party", an independent European advisory body on data protection and privacy, indicates that fines are not an ultimate remedy. It can be deduced from this that the AP is free to impose a fine, despite the fact that less far-reaching measures may be available.[13]

In this context, we also note that during a recent debate on the implementation of the GDPR, the Minister for Legal Protection indicated that the AP had assured him that it would '*focus its efforts on information and adjustment, at least in the first few years of the GDPR's application,*' and not on fining organisations that are preparing to comply with the rules. In this regard, the Minister indicated that *'we are at the beginning of a process in which many organisations and companies are busy arranging things properly.'*[14] While these may seem firm statements, it should be borne in mind that the AP is responsible for the way in which the GDPR will be enforced, and not the Minister. Therefore, these statements cannot be given too much weight and are no guarantee that the AP will not impose fines in the initial period following the entry into force of the GDPR.

The above leads to the conclusion that it will still have to become clear what standards the AP will apply when imposing fines. 'Fears' of the maximum amount of fines can perhaps be put into perspective to some extent by considering that (i) the circumstances of the specific case will play an important role in determining the amount of the fine and (ii) the AP has various other means of enforcement available.

Loss of reputation and claims for damage

Much attention is paid to the level of the fines. Something that is less obvious, but can also have significant (financial) consequences, is the risk of reputational damage as a result of non-compliance with the GDPR.

This could include, for example, damage caused by a data breach. This is the case, for example, if a (business) laptop containing personal data of third parties is stolen, if personal data becomes accessible to third parties as a result of a computer virus or a hack, but also if systems containing personal data that have not been backed up (properly) are destroyed as a result of a fire.

The GDPR contains the obligation to report data breaches to the relevant national supervisory authority and, in certain cases, also to the persons whose personal data are involved. In the Netherlands, a similar obligation has been in force since 1 January 2016.[15]

11 In short, an order subject to a penalty for non-compliance means that a penalty payment is forfeited for as long as the infringement continues – after a certain period of time has been granted to end the infringement. In the event of an administrative enforcement order, the supervisory authority will end the infringement – at the offender's expense – if the offender fails to do so within the set period.

12 Explanatory Memorandum to the Implementing Act for the General Data Protection Regulation, p. 87.

13 Article 29 Working Party: Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 of 3 October 2017.

14 House of Representatives, 59th sitting, 8 March 2018: https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/detail?vj=2017-2018&nr=59&version=2.

15 The GDPR does, however, apply a slightly different starting point with regard to reporting data breaches. Under the current law, a data breach must be reported to the AP if the data breach leads to a significant risk or serious adverse consequences for the protection of personal data. Under the GDPR, the starting point is that a data breach must be reported to the AP, unless it is unlikely that the data breach poses a risk to the rights and freedoms of natural persons. Under the current law, a data breach must be reported to the data subject(s) if the data breach is likely to have adverse consequences for the data subject's privacy. Under the GDPR, the starting point is that a data breach must be reported to the data subject(s) if the data breach is likely to pose a high risk to the rights and freedoms of the data subject(s). The Article 29 Working Party referred to above has published guidelines for determining whether such a high risk exists. If, for example, names and addresses, copies of passports or social security numbers form part of a data breach, such a high risk is deemed to exist (also in view of the risk of identity fraud).

The AP may publish the names of organisations where a data breach has occurred as part of an investigation, which may cause significant damage to the reputation of these organisations.

In addition to possible fines and the risk of reputational damage, account must also be taken of damage claims by data subjects for infringement of the GDPR. This may include claims from individuals whose data have been compromised as a result of a data breach, as well as claims from individuals who believe that they have suffered harm as a result of not being able to exercise their rights under the GDPR.

It is therefore good to bear in mind that besides the substantial fines, there are also other risks attached to non-compliance with the GDPR, which arguably are at least as significant as fines.

Recommendations

It is important to check whether the correct measures have been taken internally to ensure that your business operations are in line with the GDPR. The extensive accountability principle, which is reflected in various obligations under the GDPR, is a point of attention for many organisations.

In this context, you may think of having (and maintaining) a formal, written, internal record of processing activities, an internal policy on how to deal with personal data and how to act in the event of a data breach and a policy on retention periods.

New rights of data subjects often require adjustments to the business operations of your organisation to ensure that your organisation can meet requests of data subjects in a timely manner.

Not all obligations under the GDPR are new, but now is the time to check whether your organisation complies with the new and existing obligations concerning the protection of personal data.

About Loyens & Loeff

Loyens & Loeff N.V. is an independent full service firm of civil lawyers, tax advisors and notaries, where civil law and tax services are provided on an integrated basis. The civil lawyers and notaries on the one hand and the tax advisors on the other hand have an equal position within the firm. This size and purpose make Loyens & Loeff N.V. unique in the Benelux countries and Switzerland.

The practice is primarily focused on the business sector (national and international) and the public sector. Loyens & Loeff N.V. is seen as a firm with extensive knowledge and experience in the area of, inter alia, tax law, corporate law, mergers and acquisitions, stock exchange listings, privatisations, banking and securities law, commercial real estate, employment law, administrative law, technology, media and procedural law, EU and competition, construction law, energy law, insolvency, environmental law, pensions law and spatial planning.

loyensloeff.com

Quoted

Quoted is a periodical newsletter for contacts of Loyens & Loeff N.V. Quoted has been published since October 2001.

The authors of this issue are Jacobine van Beijeren (jacobine.van.beijeren@loyensloeff.com) and Ellen Bosma (ellen.bosma@loyensloeff.com).

Editors

You can of course also approach your own contact person within Loyens & Loeff N.V.

LOYENS & LOEFF

LOYENSLOEFF.COM

As a leading firm, Loyens & Loeff is the logical choice as a legal and tax partner if you do business in or from the Netherlands, Belgium, Luxembourg or Switzerland, our home markets. You can count on personal advice from any of our 900 advisers based in one of our offices in the Benelux and Switzerland or in key financial centres around the world. Thanks to our full-service practice, specific sector experience and thorough understanding of the market, our advisers comprehend exactly what you need.

Amsterdam, Arnhem, Brussels, Hong Kong, London, Luxembourg, New York, Paris, Rotterdam, Singapore, Tokyo, Zurich