The new EU General Data Protection Regulation and its implications for the Dutch legislation

1. Introduction

Over the last decade, cyber security has become an increasingly important issue for the organisations across the EU. Nation states and large organisations are now able to gather substantial volumes of personal information, which enables them to track individual activity in cyberspace. Digital marketing companies evolve new and more effective methods of tracking consumers. Social media companies thrive on publishing personal data. While these activities can be beneficial, it can also threaten individual privacy.[1]

The EU wants to protect the rights of individuals in respect of their personal data. After four years of preparation and debate the General Data Protection Regulation (GDPR) was finally approved by the European Parliament on 14 April 2016. On the 25th of May next year, 2018, the GDPR will replace the Data Protection Directive 95/46/EC.

[1] A. Calder, *EU GDPR*, IT Governance Publishing 2016.

The new regulation is a significant step forward in the move by elected authorities to ensure that the privacy and personal data of the EU citizens is appropriately protected. It is not only designed to protect and empower all EU citizens data privacy, but also to harmonize data privacy laws across Europe, and to reshape the way organizations across the region approach data privacy.[2] Businesses begin the process of moving to compliance with the new requirements and member states are considering the impact on national data protection legislation.

This paper gives an overview of the new GDPR, and highlights the most important aspects of the regulation. It discusses the applicability of the GDPR, the proposal for a Dutch GDPR Implementation Act, the differences between the GDPR and the DDPA, the advantages and disadvantages of the GDPR, and the steps that need to be taken in order to prepare your business for the implementation.

2. Applicability

The GDPR applies to any business that acts as data controller or data processor and that offers goods or services to individuals in the EU, regardless of whether it is physically located in the EU.[3] This potentially includes organisations everywhere in the world, regardless of how difficult it may be to enforce the Regulation. Both the data controller (likely to be within the EU) and the data processor are liable in the event of a data breach. When organisations fail to meet the regulation's requirements, severe reputational damage could incur as well as financial penalties. The regulation aims to protect information of 'natural persons, whatever their nationality or place of residence'. This means EU organisations bound by the regulation must protect personal data about anyone from anywhere in the world.

[2] Https://www.internetconsultatie.nl/uitvoeringswetavg/details.

[3] Art. 3 GDPR.

3. Proposal Dutch GDPR Implementation Act

Although the GDPR will be directly applicable in all Member States, national laws will need to be amended in order to regulate certain aspects of the GDPR. The regulation includes many open concepts and norms that need to be shaped and sharpened in practice. In the Netherlands, necessary legislative changes have already been published in the first draft national laws. On 9 December 2016, the proposal for a Dutch GDPR Implementation Act (De Uitvoeringswet Algemene verordening gegevensbescherming) was published online for the purpose of public consultation. During the public consultation period, all citizens, companies, and other institutions could submit their reactions to the proposal. This period ended on 20 January 2017. The Implementation Act will contain a legal framework for implementing the GDPR in the Netherlands. It is stated on the government website that when implementing European regulations (in general), the starting point is "policy neutrality". This means that current national law will be maintained, insofar as this is possible in the light of the specific regulation. This strategy was chosen in order to prevent the political process from reaching a deadlock, which needs to be prevented as the GDPR becomes applicable in May 2018. The Dutch Personal Data Protection Authority published a step-by-step plan for businesses to prepare for the upcoming GDPR.

- **Content of the Dutch Implementation Act**

Most interesting are the provisions relating to the position and competences of the Dutch Data Protection Authority. The role of this enforcement body is expanded. It will interact to a greater extent with international data protection authorities and has stronger enforcement powers. Other new matters include, for example, local law on profiling, special categories of personal data, rights of data subjects, and the mandatory notification of a data breach.[4] Topics where the bill also provides further specification of the GDPR

[4] De Brauw Blackstone Westbroek, *Dutch draft data protection reform bill published*, 2016.

include rules on health and education related data. The bill also provides derogative grounds such as criminal investigations and investigative powers.

- **Current status of the Dutch Implementation Act**

As mentioned before, the public consultation of the Implementation Act ended in January 2017. The Dutch government may adapt the text of the Implementation Act in the light of the submitted comments. Firstly, the Dutch government will send its definite legislative proposal to the Dutch Parliament. If the Dutch Parliament and thereafter the Dutch Senate vote to adopt it, the Implementation Act will come into force. Currently, it is unclear when and in what form the bill will be formally adopted, because it has not been sent to the parliament yet.

4. Differences between the GDPR and the DDPA

The main differences between the General Data Protection Regulation and the Dutch Data Protection Act might be unclear for businesses and organisations. Therefore, we will discuss the six most important differences in this paragraph.

1. A wider range of business activities fall within the scope of the GDPR. The central notion 'personal data' is defined more broadly in the GDPR than in the DDPA. Besides documents with names, addresses, and such like, data linked to IP addresses, MAC addresses, cookies and such like also fall under the definition of 'personal data' and within the scope of in the GDPR.

2. As mentioned before in paragraph two, the peculiarity of the GDPR is that it extends the reach of EU data protection law to non-European businesses. In particular, non-European businesses which offer goods or services to data subjects in the EU or monitor the data subjects' behaviour (provided that such behaviour takes place in the EU) will be caught and have to comply with the GDPR despite having no office or subsidiary in the

EU.[5] The DDPA, on the other hand, only applies to the processing of personal data carried out in the context of the activities of an establishment of a responsible party in the Netherlands.[6]

3. Based on the GDPR, permission from individuals is required to justify the use of their personal data. In addition, the conditions for obtaining consent have become stricter. Consent has to be unambiguous and assumed from an action.

4. The GDPR introduces a few core principles and requires businesses to show how they comply with these principles.[7] Although the principles are broadly similar to those in the DDPA, there are some new elements, such as the accountability requirement of art. 5 clause 2 GDPR.

- *First principle: lawfulness, fairness and transparency*

  The GDPR requires that the data controller provides the data subject with information about his/her personal data processing in a transparent and intelligible manner, which is easily accessible, using clear and plain language.[8]

  Transparency is achieved by keeping the individual informed and this should be done before data is collected and when any subsequent changes are made. The GDPR has a mandatory list of the information which must be given to individuals when data is obtained directly but also when it is obtained indirectly.

- *Second principle: purpose limitation*

  Processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which data was collected. Further consent is needed when the data controllers and processors want to process data

[5] Art. 3 GDPR.
[6] Art. 4 PDPA.
[7] Art. 5 GDPR.
[8] Article TaylorWessing, *The data protection principles under the GDPR*, 2016.

for another purpose later. The only exception to this requirement is where the "other purpose" is "compatible" with the original purpose.

- *Third principle: data minimisation*

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This links back to the purpose limitation.

- *Fourth principle: data accuracy*

  Personal data must be accurate and kept up to date. If data is outdated or inaccurate it should be amended or deleted.

- *Fifth principle: storage limitation*

  Businesses should delete personal data once they no longer need the data for the purpose for which it was collected, unless they have other grounds for retaining it. The GDPR requires that businesses create a regular review process with methodical cleaning of databases.

- *Sixth principle: integrity and confidentiality*

  This principle goes to the heart of protecting the privacy of individuals. Personal data must be protected against unauthorised access, accidental loss, destruction or damage. There should be policies in place to review the security of the data on a regular basis and to make updates if required.

- *Seventh principle: accountability*

  The new accountability principle in article 5 clause 2 of the GDPR requires businesses to demonstrate compliance with the principles of the GDPR. Article 24 of the regulation sets out how organisations can do this by requiring the implementation of appropriate technical and organisational measures to ensure that businesses can demonstrate that the processing of personal data is

performed correctly.[9] One of the biggest changes under the GDPR compared with the DDPA, is this increased compliance burden, much of which is sparked by this principle.

5. The GDPR creates some new rights for individuals and strengthens some of the rights that exist under the DDPA.

- The right to data portability – art. 20 GDPR; allows individuals to obtain and reuse their personal data for their own purposes across different services.
- The right to object – art. 21 GDPR; enables individuals to object to specific types of processing: direct marketing, processing based on legitimate interests or performance of a task in the public interest/exercise of official authority, and processing for research or statistical purposes.
- The right to erasure – art. 17 GDPR; enables individuals to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- The right to restrict processing – art. 18 GDPR; ensures that, when processing is restricted, businesses are permitted to store personal data, but are not allowed to process it further.

6. In the case of a personal data breach, the data controller has to report the data breach to the Data Protection Authority not later than 72 hours after having become aware of it. They also have to maintain an internal breach register. In contrast with the DDPA, businesses are obliged to document data breaches under the GDPR, even when these breaches do not have to be reported to the Data Protection Authority.

[9] NYMITY, *Accountability Roadmap for Demonstrable GDPR Compliance,* 2017.

5. Advantages & disadvantages of the GDPR

The biggest advantage of the GDPR is the potential harmonisation of fragmented regulations. Up to now, businesses had to take account of regulations on data protection of 28 different member states. The GDPR will soon provide one legal framework that is applicable throughout Europe. This will be beneficial to small and medium sized businesses in case they wish to expand abroad, because they only have to take account of one legal framework instead of several legal frameworks. It will save time and resources. Recent estimates of the European Commission show that businesses could save up to 2.3 billion euros per year thanks to the GDPR.[10]

Bridget Treacy, partner and head of UK privacy and cyber-security at law firm, Hunton & Williams thinks that businesses will have to adapt and improve their data management at high speed in order to comply with the legislation. She welcomes the new rules:

"It enhances consumer rights and means businesses are going to have to focus on making sure they know what data they've got and what they do with it. One of the requirements of the legislation is that companies only collect the minimum amount of data that they require for a specific purpose. Firms are going to have to be much clearer about what data they are collecting and why. It means that they will not be able to hold on to data as a bit of a comfort blanket," she said.[11]

Despite the advantages, the GDPR has been criticised as well. One of the painful areas has to do with the fact that a regulation is a European law that is fully and directly applicable in all member states. The GDPR contains provisions which leave room for multiple interpretations. A different approach by member states, motivated by culture and supervisor's priorities, is not unthinkable. As a result, the extent to which the GDPR will achieve its harmonisation scheme is uncertain.

[10] London Economics, *Implications of the European Commission's proposal for a general data protection for business*, 2013.
[11] BBC News, *Critics condemn new EU data-protection legislation*, Technology 2013.

The European technology industry trade group DigitalEurope has long criticized the legislation, arguing it covers too many types of data and fails by not making meaningful distinctions between things like a person's name and country of origin and far more sensitive data like medical records and voting history.

"We believe that the final text fails to strike the right balance between protecting citizens' fundamental rights to privacy and the ability for businesses in Europe to become more competitive," DigitalEurope director general John Higgins said in a statement.[12] Despite this statement, he also said it is time to be pragmatic and DigitalEurope stands ready to make the new legal framework for date protection in Europe work.[13]

6. Preparing for the GDPR

If you are an entrepreneur, there are a few steps that you and your business need to take in order to be well prepared for the GDPR on time.[14]
You should take the following steps:

- Document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit. Documenting the personal data will help you to comply with the accountability principle, which requires businesses to be able to show how they comply with the data protection principles we have discussed in Chapter 4 (point 4);

- Review your current privacy notices and put a plan for making any necessary changes in time for GDPR implementation. Article 12, 13 and 14 of the GDPR show data controllers have to give privacy information to data subjects. This is done through a privacy notice. The information about how your business processes

[12] K. Finley, *EU cracks down on data privacy, but loopholes may remain*, Wired Business 2016.
[13] DigitalEurope, *EU Data Protection Reform: Implementation of the GDPR needs active involvement of industry*, 2016.
[14] ICO., *Preparing for the GDPR*, 2017.

personal data must be concise, transparent, easily accessible, written in clear and plain language, and free of charge.

- Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. As we have discussed before, the GDPR gives individuals some new rights, such as the right to data portability, the right to object, the right to erasure, and the right to restrict processing.[15]

- Identify the lawful basis for your processing activities in the GDPR, document it and update your privacy notices to explain it. Where consent is the basis for processing, you should review existing mechanisms for obtaining consent, to ensure that they meet the GDPR's standards. Where a legitimate interest is the basis for processing, you should maintain records of the businesses' assessment of that legitimate interest, to show that the business properly considered the rights of data subjects. Documenting your lawful bases is important in order to help you comply with the accountability requirements.

- Review how you seek, record and manage consent and whether you need to make any changes. Consent must be freely given, specific, informed and unambiguous. You will have to delete existing consents if they do not meet the GDPR standard.

- Make sure you have the right procedures in place to detect, report and investigate a personal data breach. As mentioned before, the GDPR requires notification of a breach by the data controller to the relevant supervisory authority without undue delay, and with a written explanation for the reasons behind any response later than 72 hours after discovery. To do this successfully involves having the right

[15] Chapter 4, point 5, of this article.

sort of controls in place, an essential requirement of GDPR, that give you the capacity to detect and respond to security events.

- Designate someone to take responsibility for data protection compliance and assess where this role will sit within your businesses' structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

- Determine your lead data protection supervisory authority if your business operates in more than one EU member state. Article 29 Working Party guidelines could help you do this. The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

7. Conclusion

The GDPR is a significant step forward in the move by authorities to ensure that the privacy and personal data of the EU citizens is appropriately protected. Businesses begin the process of moving to compliance with the new requirements and member states are considering the impact on national data protection legislation. National laws will need to be amended in order to regulate certain aspects of the GDPR. On 9 December 2016, the proposal for a Dutch GDPR Implementation Act was published and consulted by the public. However, it is currently unclear when and in what form the bill will be formally adopted, because it has not been sent to the parliament yet.

The biggest advantage of the GDPR is the potential harmonisation of fragmented regulations. Up to now, businesses had to take account of regulations on data protection of 28 different member states. Despite several advantages, the GDPR has been criticised as well. The GDPR contains provisions which leave room for multiple interpretations. A different approach by member states, motivated by culture and supervisor's priorities, is

not unthinkable. As a result, the extent to which the GDPR will achieve its harmonisation scheme is uncertain.

There are a few differences between the General Data Protection Regulation and the Dutch Data Protection Act. It is important for Dutch businesses to be aware of these differences. Being aware of the fact that the law is changing, is the first step in moving towards compliance. It is essential to plan an approach and follow the steps mentioned in chapter six of this article.

Contact

If you have questions or comments after reading this article, please feel free to contact mr. Maxim Hodak, attorney-at-law at Law & More via maxim.hodak@lawandmore.nl, or mr. Tom Meevis, attorney-at-law at Law & More via tom.meevis@lawandmore.nl, or call +31 (0) 40-36 90 680.

**Please note that this publication only acts as an informative document. No rights can be derived from it. Actions should not merely be based on the content of this publication.*