The General Data Protection Regulation applicable as of 25 May 2018

The General Data Protection Regulation (full name: *Regulation 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*, hereafter: the "**Regulation**") entered into force on 24 May 2016 and will become effective as from 25 May 2018. The Regulation will repeal the current legal framework of data protection in Europe which is based on the Directive 95/46/EC (hereafter: the "**Directive**") which was implemented in the Member States in different ways, resulting in a fragmented level of protection.

The data protection reform is aimed at strengthening the rights of the persons, whose data are processed ("**data subjects**"), by replacing the current system of various national laws with a unified system of data protection, which will be applicable anywhere in the EU. It is also aimed at simplifying the regulatory environment for businesses by providing them with only one set of rules and lightening the administrative burden and facilitating the interactions with data protection regulators by introducing a one-stop shop for multi-jurisdictional companies.

Due to the direct effect of the EU Regulations in the Member States, it will be immediately applicable in all EU Member States, including the Netherlands. It will apply automatically and will not require any national implementation by the Member States. As a result, the currently applicable Directive will be repealed and the Regulation will apply instead of the current national legislation of the Member States implementing the Directive. The Dutch Data Protection Act (*Wet bescherming persoonsgegevens*, the "**DPA**") will entirely be repealed by the Dutch Legislator. The Regulation will therefore have important consequences not only for natural persons but also for businesses.

The Netherlands have already implemented some of upcoming changes which will be introduced by the Regulation. On 1 January 2016 the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) was amended, bringing about some substantial changes to the Dutch data protection legislation. The Amendment introduced an obligation for controllers to report data breaches and expanded the enforcement powers of the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) by adding a power to issue penalties in case of non-compliance with this new obligation. These recent amendments to the DPA anticipate the more extensive obligations of the controllers and processors that will apply under the Regulation.

Substantive scope

The substantive scope of the Regulation is similar to the current Directive, with some exceptions.

The Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of thereof (Article 2). Some limitations of the scope apply, such as use of the data by a natural person in the course of a purely personal or household activity.

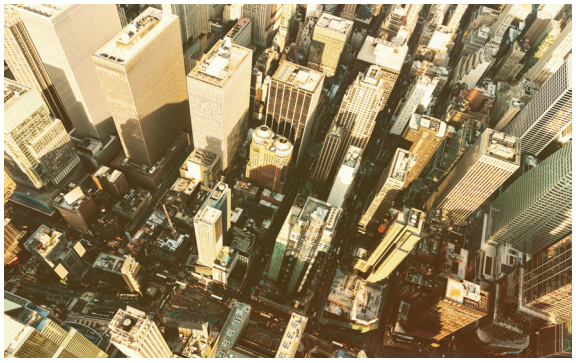
Also the definition of personal data remains largely the same. Any information relating to an identified or identifiable natural person is considered personal data, with addition of online identifier and location data as possible ways to identify a person (Article 4). The definition of the special category of sensitive data now in some cases includes genetic and biometric data (Article 9).

One important change in scope is that the Regulation will now apply to controllers (the (legal) person or body determining the purpose and means of the data processing) as well as processors (the (legal) person or body which processes the personal data on behalf of the controller). The Regulation also introduces specific legal obligations for processors, such as maintaining records of processing activities and processed data (Article 28, 32). The Regulation further introduces a broader accountability and responsibility of processors. The introduction of new obligations for processors does not, however, relieve the controllers of their obligations or responsibilities if the processor is involved. Controllers retain their obligations and have to ensure that their contract with the processor is in full compliance with the Regulation.

Territorial scope

The territorial scope of the data protection rules becomes particularly broad under the Regulation.

Firstly, the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the EU or not (Article 3). The definition of "establishment" remains the same as under the current Directive (number) and means effective exercise of activities regardless the legal form of the establishment.



Secondly, the Regulation will also apply to controllers or processors without an establishment in the EU if: (a) they offer goods or services to data subjects in the EU, irrespective of whether a payment is required; or (b) they monitor the behavior of the data subjects within the EU. In case these activities take place, a controller or processor is obliged to designate a representative in the EU (Article 27).

Responsibilities of controllers and processors

The controllers must implement appropriate technical and organizational measures to ensure security of personal data and implement appropriate data protection policies. The controllers must be able to demonstrate that processing is performed in accordance with the Regulation (Article 24).

The provision on "Privacy by Design" requires that, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the data processing, the controller shall implement appropriate technical and organizational measures into each new business process or service that processes of personal data to protect the personal data. "Privacy by Default" requires the highest privacy setting to automatically apply when a customer acquires a new product or service. No action on the side of the data subject should therefore be necessary for the highest privacy setting to apply (Article 25).

Automated decision making, including profiling could be contested by the data subjects under the Regulation. The data subjects have a right not to be subject to a decision based solely on automated processing, which produces legal effects concerning them or significantly affect them (Article 22). Furthermore, the data subject has the right to be forgotten (the right to obtain from the controller the erasure of personal data concerning him or her without undue delay) (Article 17).

If data processing is likely to result in high risks to the rights and freedoms of data subjects (Article 35), data protection impact assessments have to be conducted prior to processing. The impact assessments have to be conducted in consultation with the supervisory authority.

Companies which regularly and systematically monitor data subjects on a large scale or process particular categories of data, are obliged to designate a data protection officer (Article 37).

Consent

All data processing must be based on explicit consent of the data subject (Article 7). The consent of the data subject must be freely given, specific, informed and unambiguous. The controller must be able to demonstrate that consent has been given and the data subject retains the right to withdraw the consent.

Enforcement

The national supervisory authorities ("**SA**") will be tasked with enforcement of compliance with the Regulation (Article 51). Every EU Member State currently has a data protection authority. In the Netherlands this is the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, "**DPA**"). The current data protection authorities will likely be transformed into the SA's for the purposes of the new Regulation.

The penalties for non-compliance, which now vary depending on the country, will be determined by the Regulation and amount to a maximum of EUR 20,000,000 or 4% of the total worldwide annual turnover, whichever is higher.

One Stop Shop

If a company is established and operates in many jurisdictions, there is a possibility that various national SA's will have different interpretations of the legal framework applicable to this company. To avoid this risk a so-called "One Stop Shop" will be introduced under the new Regulation. A multi-jurisdictional company will be assigned a "lead authority", depending on the place of its main establishment in the EU. The lead authority consults and cooperates with all other SA's where the company operates to supervise the processing activities of the company (Article 60). If the relevant authorities agree on a certain decision, the lead authority will adopt it and this decision will be binding on all relevant SA's.

The controller or processor will then have to comply with this decision in all its locations in the EU.

An obligation to report data breaches

The general obligation to report data breaches, already introduced in the Netherlands as of 2016, will remain largely the same under the new framework. The data breach has to be reported to the competent SA in all cases. The controller has to report the breach without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. Notification made at a later time must be accompanied by reasons for the delay. In case the breach is likely to result in a risk to the rights and freedoms of the data subject, the breach has to be reported to the data subject (Article 33). The processor is obliged to notify the controller of the data breach as soon as possible. The notification to the SA must include the nature of the personal data breach, the name and contact details of the data protection officer and description of the likely consequences.

Further remarks

The Regulation will introduce a uniform data protection framework across the EU. It should be noted, however, that Member States may impose additional obligations and allocate other tasks to the national SA's. Also the civil proceedings will take place before national courts, which may presumably apply or seek inspiration in the existing body of national case law.

From the practical point of view it is important for organizations to ensure that a privacy compliant framework is in place, including technical safeguards, such as pseudonymisation or encryption, as well as sound privacy policies. It is further important to keep thorough documentation which allows the organization to demonstrate that processing is performed in compliance with the Regulation.

Key contacts

Philip ter Burg
Partner
p.terburg@burenlegal.com
T +31 (0)70 318 4828

Larissa Bogers
Associate
l.bogers@burenlegal.com
T +31 (0)70 318 4200

The information in this publication is for general information purposes only and does not claim to be comprehensive or provide legal or other advice.
Buren N.V. accepts no responsibility for loss which may arise from accessing or reliance on information contained in this publication.