1 LEGAL FRAMEWORK

1.1 The Dutch Act on the Protection of Personal Data and the General Data Protection Regulation

In the Netherlands, the processing of personal data is subject to the Act on the Protection of Personal Data (the “APPD”), which implements EU Directive 95/46/EEC. This directive was generally considered unfit to deal with the protection of personal data in an era of exponential growth of data and technology. As a result, the EU decided to replace the current law with a new General Data Protection Regulation (EU Regulation 2016/679; the “GDPR”). The GDPR will enter into effect on 25 May 2018 and will replace the APPD.

The GDPR will have a substantial impact on all IT and business processes of EU-based companies as well as non-EU companies directing their activities at the EU. The GDPR contains a multitude of new requirements, a generally more strict approach to data governance and a serious sanctions regime.

The purpose of this memorandum is to provide only a high level overview of the legal framework on privacy and data protection in the Netherlands and the most important changes introduced by the GDPR.

This memorandum was last updated on 10 November 2017.
2 MATERIAL AND TERRITORIAL SCOPE OF APPLICATION

2.1 Definitions

**Personal data**
Personal data are any information relating to an identified or identifiable natural person (also referred to as the data subject). An identifiable natural person is one who can be identified, directly or indirectly, for instance via a name, an identification number, location data, photographs or an IP address. The European Court of Justice and Data Protection Authorities ("DPAs") across Europe have developed a highly dynamic interpretation of the "personal data" concept and are quick to include new types of data within its definition, such as dynamic IP addresses and cookies.

**Sensitive data**
Sensitive data are personal data that reveal racial or ethnic origin, political opinions, sexual preferences, religious or philosophical beliefs, or trade union membership. The processing of these data is prohibited, unless strict exceptions (e.g. explicit consent) apply.

**Processing**
Processing means any operation or any set of operations concerning personal data, such as collection, recording, organisation, structuring, storage, adaptation, erasure or destruction.

**Controller**
The data controller is the natural person, legal person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal data.

**Processor**
The data processor is the person or body which processes personal data for the data controller, without coming under the direct authority of that party (e.g. a cloud service). Pursuant to the APPD, the primary obligation to comply with EU data protection law falls on controllers. In addition, the GDPR imposes direct legal obligations on processors. Moreover, like controllers, processors can be held liable for payment of administrative fines and penalties under the GDPR.
2.2 Territorial scope of application

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a company (controller or a processor) in the EU, as well as in the event that the processing does not take place in the EU (e.g. a cloud services that uses non-EU subcontractors to perform part of the processing). Furthermore, it also applies to companies (controller or processor) established outside the EU if they: (i) offer goods or service to individuals in the EU; or (ii) monitor the behaviour of individuals in the EU.
3 ADMINISTRATIVE FINES AND ENFORCEMENT

**Administrative fines under the APPD**
Currently, the Dutch Data Protection Authority can impose an administrative fine of maximum EUR 820,000 for violations of the APPD. This fine can be increased for legal entities to up to 10% of the company’s annual net turnover, although the Dutch DPA has expressed it does not expect to use this latter authority. As of 25 May 2018, the fines of the GDPR apply across Europe.

**Extension of enforcement powers under the GDPR**
Sanctions and penalties will significantly increase under the GDPR, and the competent DPAs will be given wide-ranging powers to enforce compliance with it. Companies that do not comply with the GDPR can be subjected to fines of up to EUR 20,000,000, or 4% of the annual worldwide turnover for certain violations, whichever is higher. Companies can also be placed under regular DPA audits. The eventual amount of a fine will depend on various criteria, including the severity and duration of the violation, whether it was intentional or not, and any mitigation measures, nature of the personal data, level of cooperation with DPA and history of compliance.

**One DPA**
Under the GDPR, a company may choose one single DPA as its lead authority, based on the location of its main establishment within the EU. This authority will supervise all the processing activities of that business. The lead DPA must consult other DPAs in case its actions affect processing activities in other EU member states.
4 OBLIGATIONS FOR CONTROLLERS AND PROCESSORS

4.1 General principles

There are several general principles that must always be observed. Companies must process personal data lawfully, fairly and in a transparent manner. Personal data may only be collected for specified, explicitly defined and legitimate purposes and may in principle not be held in a manner that renders identification of the data subject possible for any longer than required for the purpose of the processing. Moreover, personal data must be accurate and may only be processed in so far as relevant, adequate and limited to the purpose for which they are processed. Finally, personal data must be processed in a manner that ensures appropriate security of the personal data.

Processing must be based on one of the processing ground mention in data protection legislation. Under the GDPR, processing is lawful when it fulfils one of the criteria set out in article 6, such as processing being necessary to comply with a legal obligation, to protect the vital interests of the data subject or when a controller has a legitimate interest. In most cases, however, processing will only be lawful when the data subject has given its consent to the processing.

4.2 Consent

Under the GDPR, the consent of a data subject will become harder to rely on. Consent should be explicit and may in principle not be a condition for the execution of the contract or provision of the service. Consent must be presented in a clearly distinguishable manner from other matters in an intelligible and easily accessible form, using clear and plain language. Withdrawing consent must be equally as easy as giving consent. The European Data Protection Working Party (also referred to as the Article 29 Data Protection Working Party, “WP29”) has yet to publish guidelines on consent, which we expect to provide further guidance on how to obtain consent from data subjects in practice.

4.3 Data protection by design and by default

The principles of data protection by design and default require that data protection safeguards should be built into products and services from the earliest stage of development. Privacy-friendly default settings should be the norm.
4.4 Data processing agreement

In the event data is processed on behalf of and upon the instruction of the controller by a processor, a data processing agreement has to be concluded containing certain conditions prescribed by the GDPR, such as that the processor must delete or return personal data upon request of the controller.

4.4.1 Demonstrating compliance (accountability)

Controllers must be able to demonstrate compliance with the GDPR by adopting compliance programs. These should include the following elements: (i) rolling out relevant data protection, data retention and data security programs, (ii) appointing a Data Protection Officer (the “DPO”, see below), (iii) implementing information security measures (see below), and (iv) maintaining internal records of data processing activities.

DPO

Controllers or processors must appoint a DPO when the core activities involve regular and systematic monitoring of individuals or involve large scale processing of data in the special categories. The DPO must have specific knowledge of data protection law and must, among other things, advise the business on its compliance obligations.

Information security measures

The controller and the processor have the obligation to take adequate technical and organisational security measures to protect the data against loss or unlawful processing. Technical measures include, for instance, protection by means of encryption and a password. Organisational measures include, among others, only providing access to the data to a limited number of individuals, who are bound by a confidentiality obligation.

4.5 Data breach notification

Under the GDPR, processors need to report data security breaches to controllers, who in turn need to report data security breaches to the competent DPA and – in case of a high risk to the rights and freedoms of individuals – to the affected individuals.

The controller must notify the DPA without undue delay of a data security breach, with the presumption that 72 hours after detection of such a breach by the processor constitutes “without undue delay”. The data breach notification obligation is already in place in the Netherlands, effective 1 January 2016.

4.6 Data Protection Impact Assessments

Where processing operations (e.g. in view of a new business process or product) result in a high risk to the rights and freedoms of individuals, companies should carry out data
protection impact assessments ("DPIAs") to assess the privacy risks to individuals. Where a DPIA reveals risks to the privacy of the individual, it should identify measures to address these risks.

4.7 Profiling

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

The natural person has the right to object to profiling and must always be informed about this right. The GDPR limits profiling to cases where the natural person has given his explicit consent, when necessary for a contract with the company, or is authorised by EU or domestic law to which the controller is subject. The GDPR prohibits decision-making based solely on automated processing of sensitive data, unless companies can rely on one of the legal bases available for the processing of sensitive data.

Even though the WP29 is still working on guidelines on consent, it has already set out some ways of obtaining consent regarding profiling:

(a) provide sufficiently clear and comprehensive information about the profiling to ensure individuals understand what they are consenting to;

(b) introduce a process of granular consent where individuals are provided with a clear and simple way to agree to different purposes of processing;

(c) actively seek consent from individuals before any new processing takes place; and

(d) inform the data subject that they can withdraw consent.
5 DIRECT MARKETING

Data protection requirements for direct marketing are set out in Directive 2002/58/EC on privacy and electronic communications, which has been implemented by amendments to the Dutch Telecommunications Act (the “TA”). Currently, the EU is considering a revision of these rules and adopting new legislation that has immediate binding effect across Europe, popularly known as the ‘E-Privacy Regulation’. If your company is conducting direct marketing activities, you should closely monitor these developments.

**Conditions for sending direct marketing e-mail (opt-in)**
The TA provides that the use of e-mail to transmit unsolicited communications for commercial, idealistic or charitable purposes is only permitted if the sender can demonstrate that the subscriber concerned has provided his prior consent.

**Exemptions (opt-out)**
The TA provides that a recipient of the electronic contact details may use those details to transmit communications for commercial purposes where:

(a) it has received the data in the context of the sale of its products or services;

(b) the commercial communication relates to its own similar products or services; and

(c) at the time of receipt of the contact details, the customer is clearly and expressly offered the opportunity to object to the use of such electronic details, and, where the customer does not object to this use, the customer is clearly and expressly offered the opportunity to object to further use of his electronic contact details in each transmitted communication.
6 RIGHTS OF THE DATA SUBJECT

6.1 Right to information

Currently under the APPD, the controller must provide the data subject with the following information prior to obtaining the personal data, unless the data subject is already acquainted with this information:

(a) the identity of the controller;

(b) the purposes of the data processing;

(c) other relevant information, such as for example the identity of recipients of the data, and the nature of (the categories of) personal data processed; and

(d) in the event of transfer of data to a country outside the EEA, on the fact that this is occurring and for what purposes, as well as the level of protection offered by the relevant country.

A higher standard of information notice will be required under the GDPR. Next to the requirements above, the notice must be more detailed and should include, among other information:

(a) the identification of the DPO;

(b) data retention periods; and

(c) an explanation of the right to data erasure and the right to object to data processing.

Furthermore, information notices should be transparent and easily accessible.

6.2 New data subjects’ rights

The APPD already provides for the right of access, rectification and right to object. Under the GDPR data subjects gain “new” rights which are (i) the right to erasure or (ii) the right to restrict processing of personal data, and (iii) the right to data portability. An overview of these rights is provided below.

Right of access

The data subject has the right to obtain from the controller a full and clear overview of (among other information) the purposes of the processing, the categories of processed
data and the (categories of) recipients, as well as the existence of the right to request rectification or erasure of personal data.

**Right of rectification**
Data subjects have the right to obtain from the controller rectification of inaccurate personal data.

**Right to object**
The data subject has the right to object if the processing of his personal data is necessary for (i) the proper performance of a public law duty performed by an administrative body, (ii) the legitimate interests of the controller or a third party.

**Right to erasure**
Individuals can request controllers that process their data to erase any links to, or copy or replication of, their data. In such a case, the company should now inform any recipients of such data that they must also delete the personal data.

**Right to restrict processing of personal data**
Under certain circumstances the individual can ask the company to restrict the processing of his personal data.

**Right to data portability**
The GDPR entitles individuals to request transmission of their personal data from one data controller to another data controller, and to receive personal data concerning them in a structured, commonly used and machine-readable format.
7 TRANSFER OF PERSONAL DATA

7.1 Within the EEA

The transfer of personal data within the EEA is permitted, as all countries within the EEA provide an adequate level of protection.

7.2 Outside the EEA

A limited number of countries, such as Israel and Switzerland, are seen as having an adequate level of protection and are thus treated as EEA country (see para. 7.1). For most countries outside the EEA, controllers must put in place appropriate safeguards. For example, a legally binding instrument between public bodies or including the Standard Contractual Clauses adopted by the European Commission in an agreement between contracting parties.

Privacy Shield Framework

In the case of US recipients, the adherence to the “Privacy Shield Framework” may permit transfer of personal data to the US. However, as the Privacy Shield Framework is under heavy scrutiny by regulators and may be invalidated in the future, it is advisable to have mechanisms in place to cater for alternative transfer mechanisms in such case. The Privacy Shield Framework is currently under review by the WP29.

New data transfer mechanisms

Under the GDPR, Binding Corporate Rules (“BCRs”), codes of conduct or certification schemes will be explicitly recognised as a data transfer mechanism. Data exporters will no longer be required to obtain additional approval from DPAs for transfers based on the BCRs.
8 EXPERTS

RICHARD VAN STADEN TEN BRINK
Partner
richard.brink@debrauw.com
T +31 20 577 1922

AXEL ARNBAK
Senior Associate
axel.arnbak@debrauw.com
T +31 20 577 1973

De Brauw Blackstone Westbroek
Claude Debussylaan 80
1070 AB Amsterdam
The Netherlands

www.debrauw.com