HOUTHOFF

STEPS TOWARDS GDPR COMPLIANCE

THE GDPR: WHAT IT MEANS

As of 25 May 2018, the new EU General Data Protection Regulation (Regulation 2016/679, or "GDPR") will provide a new legal framework for privacy and data protection in the European Union. The GDPR will replace the 1995 Data Protection Directive, which is transposed into each EU member state's national laws. While the GDPR resembles the principles of the Data Protection Directive, it has some important new key elements.

This brochure describes the new key elements of the GDPR, the GDPR's data processing principles and the steps that an organisation should take towards compliance with the GDPR.

NEW KEY ELEMENTS

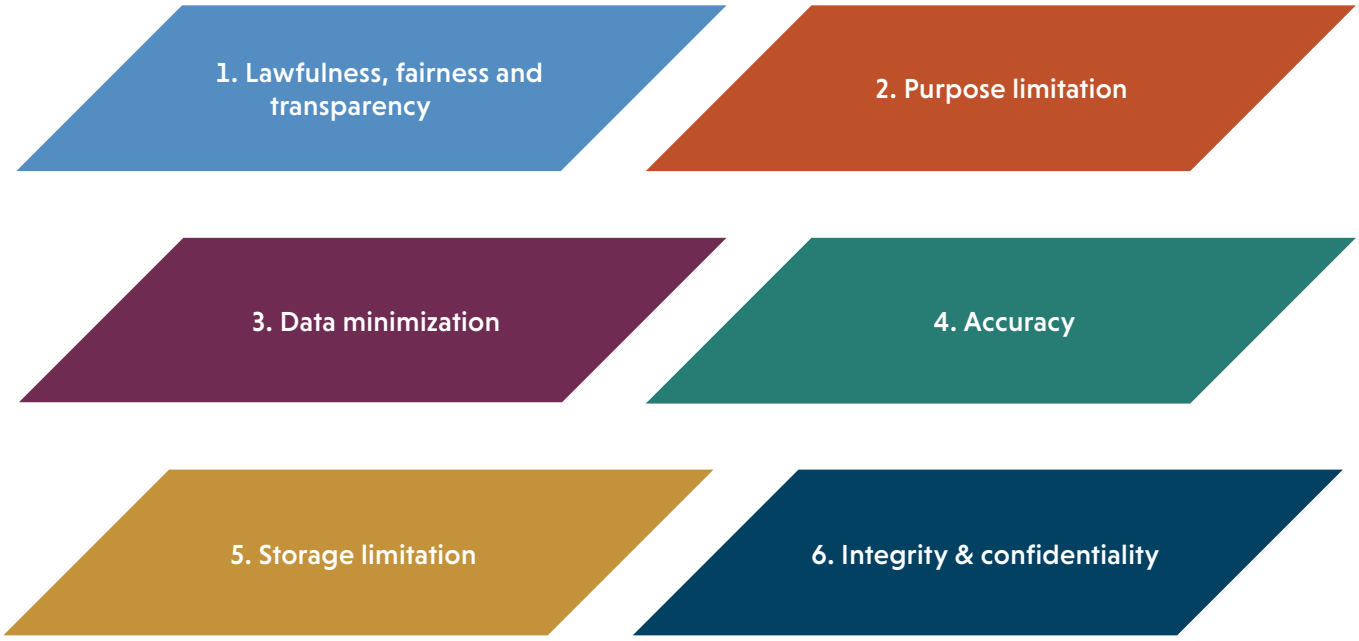
- Fines for non-compliance of up to 20 million euros or 4% of your organisation's global annual turnover
- New rights for data subjects, such as 'the right to be forgotten' and 'data portability'
- Data breach notifications
- Data Protection Impact Assessments (DPIAs)
- Additional requirements for engaging data processors
- Privacy notices: additional information requirements
- Extended transparency requirements towards data subjects
- Accountability: requirement to demonstrate compliance with the GDPR

APPLICABILITY TO ORGANIZATIONS OUTSIDE THE EU

The GDPR expands the territorial scope of EU data protection legislation. The GDPR applies to the processing of personal data by an establishment of a controller in the EU in line with the 1995 Data Protection Directive. In addition to this, the GDPR will also apply to organisations established outside the EU that offer goods or services to data subjects in the EU, or monitor behaviour of data subjects in the EU.

THE GDPR'S DATA PROCESSING PRINCIPLES

The GDPR relies on a few core principles which set out what organisations should do when processing personal data.



1. Lawfulness, fairness and transparency
Personal data shall be processed fairly and lawfully in a transparent manner in relation to the data subject.

2. Purpose limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data minimization
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the personal data are processed.

4. Accuracy
Personal data shall be accurate and, where necessary, kept up to date.

5. Storage limitation
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed.

6. Integrity & confidentiality
Technical and organisational measures shall be taken to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

ACCOUNTABILITY

The controller is responsible for, and must be able to demonstrate compliance with, the above data processing principles. This means that organisations are expected to implement technical and organisational measures, including, for example, internal data protection policies, internal audits of processing activities and data breach protocols.

STEPS TOWARDS GDPR COMPLIANCE

The GDPR describes how organisations should comply with its principles. We advise organisations to take the following steps towards compliance with the GDPR.

1

Data mapping
Identify and understand the personal data flows to, from and within your organisation, to get an overview of the personal data processing activities within your organization.

2

Maintain a data processing register (where applicable)
The GDPR requires most organisations to keep a record of their personal data processing activities. This requires you to document what personal data you hold, what you do with the personal data and with whom you share the personal data.

3

Determine data retention periods
Personal data should generally only be retained for as long as necessary for the purpose(s) for which the data are used. The actual retention period may vary based on the different categories of personal data that are processed. For example, the retention period for personal data of job candidates differs from and is generally shorter than the retention period regarding personal data included in tax declarations. Organisations are advised to implement a data retention policy specifying a retention period for each category of personal data.

4

Conduct a DPIA (where required)
Organisations may be required to conduct a Data Protection Impact Assessment (DPIA) prior to the processing of personal data, where the processing (in particular using new technologies) is likely to result in a high risk to individuals. A DPIA allows organisations to identify possible privacy risks and take measures to eliminate or mitigate those risks.

5

Conclude data processing agreements
When an organisation (a controller) engages a third party for the provision of services (such as hosting or payroll services), such third party may process personal data as a processor, on behalf of the controller. In that event, the GDPR requires this organisation to make written arrangements with the processor it engages for the processing of its personal data.

6

Implement a data breach protocol
The GDPR requires organisations to report personal data breaches to the competent data protection authority within 72 hours after discovery of such personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. In order to respond timely and adequately, it is advised to implement a data breach protocol that enables organisations to effectively detect, investigate and report personal data breaches.

7

Privacy by design & privacy by default
When developing new products, services or processes which involve the processing of personal data, the GDPR's data protection principles should be taken into account. In addition, the default settings for these new products, services or processes should be 'privacy friendly'.

8

Appoint a Data Protection Officer (DPO) (if required)
Organisations may be required to appoint a DPO. In any event, a DPO must be appointed if (i) the processing is carried out by a public authority; (ii) data subjects are systematically monitored; or (iii) special categories of personal data are processed on a large scale.

9

Update information notices / privacy statements
Organisations are obliged to inform data subjects (e.g. employees, customers, patients) about the processing of their personal data. Data subjects are usually informed through information notices, such as a privacy statement. The GDPR contains an extensive list of information that must be provided.

10

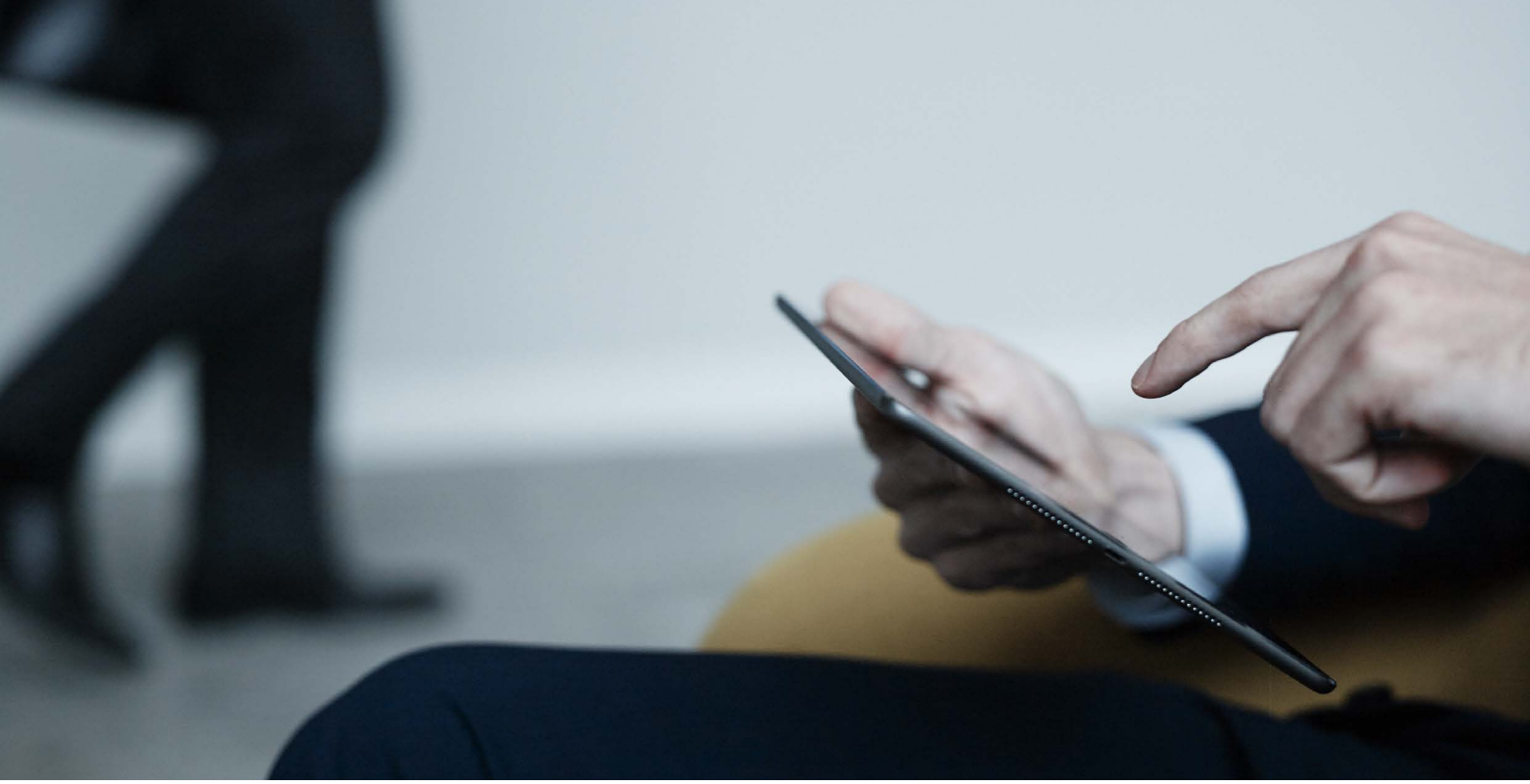
Check consent forms
Review how your organization obtains consent. Under the GDPR, consent must be freely given, specific, informed and unambiguous in order to be valid. Data subjects should further be able to withdraw their consent at any time and the controller must be able to demonstrate that consent has been given.

11

Data subjects' rights
Organizations should take the necessary technical and organizational measures to be able to comply with data subjects' requests and queries, such as access requests, and requests for the erasure, portability or rectification of personal data. Organizations are advised to verify and where necessary update their internal procedures in order to comply with requests of data subjects.

12

Establish your lead supervisory authority
If your organisation operates in more than one EU member state or is engaged in forms of cross-border processing, it may be able to benefit from the one-stop-shop principle. This means that one single lead supervisory authority may be competent. Controllers should assess the applicability of the GDPR's one-stop-shop mechanism and the allocation of the lead supervisory authority within their group.



CONTACT

Houthoff's Privacy & Data Protection Team has broad experience in assisting clients to achieve compliance with the GDPR. The team regularly conducts GDPR compliance projects and privacy audits for clients. The team has particular experience in working on complex data protection matters and projects for clients in the automotive, ecommerce, retail, financial services and construction sectors.

THOMAS DE WEERD
ADVOCAAT | PARTNER
T +31 20 605 69 85 | M +31 6 5165 9208
t.de.weerd@houthoff.com

JAN BRÖLMANN
ADVOCAAT | SENIOR ASSOCIATE
T +31 20 605 65 94 | M 31 6 4704 3567
j.brolmann@houthoff.com

JURRE REUS
ADVOCAAT | ASSOCIATE
T +31 20 605 65 76 | M +31 6 8380 3239
j.reus@houthoff.com

@HouthoffPrivacy