

## 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 in the GDPR, the GDPR’s data processing principles and the steps an organization should take towards compliance with the GDPR.

#### NEW KEY ELEMENTS

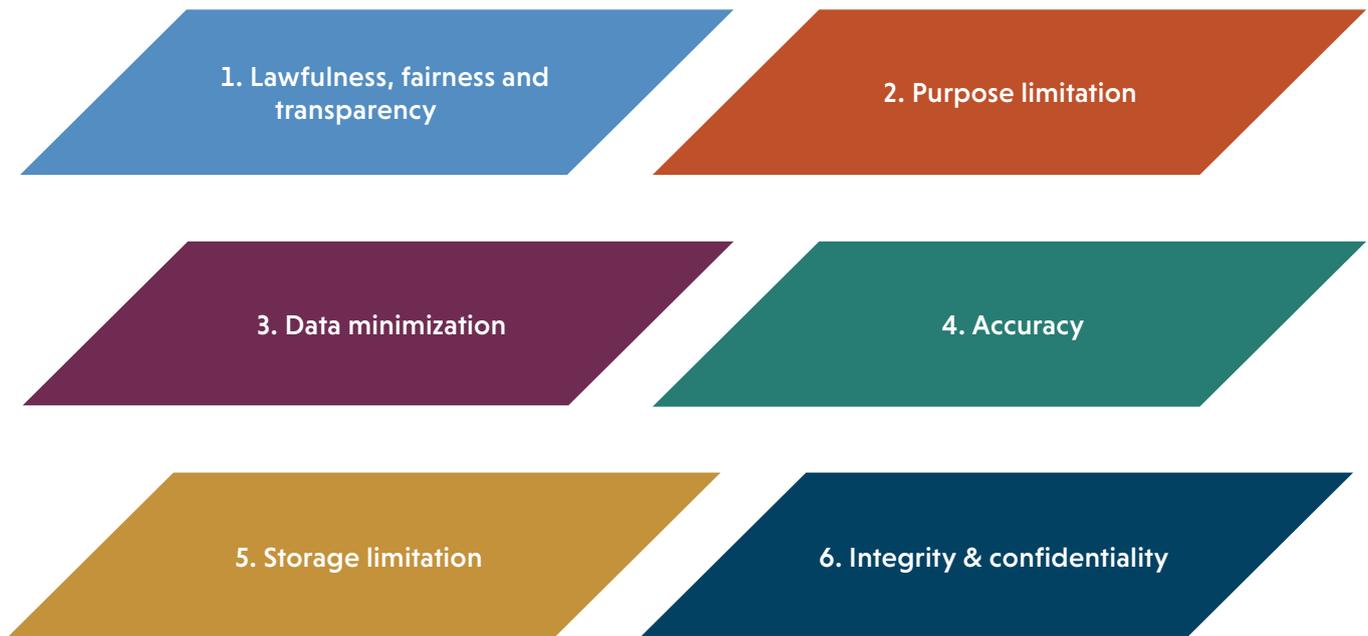
- Fines for non-compliance of up to 20 million Euros or 4% of your organization’s global annual turnover
- New rights for data subjects, such as ‘the right to be forgotten’ and ‘data portability’
- Data breach notifications
- Data Protection Impact Assessments (DPIAs)
- Additional requirements for engaging 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. In line with the 1995 Data Protection Directive, the GDPR applies to the processing of personal data by an establishment of a controller in the EU. In addition to this, the GDPR will also apply to organizations established outside the EU that offer goods or services to data subjects in the EU, or monitor behavior of data subjects in the EU.

## THE GDPR'S DATA PROCESSING PRINCIPLES

The GDPR relies on a few core principles which set out what organizations 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

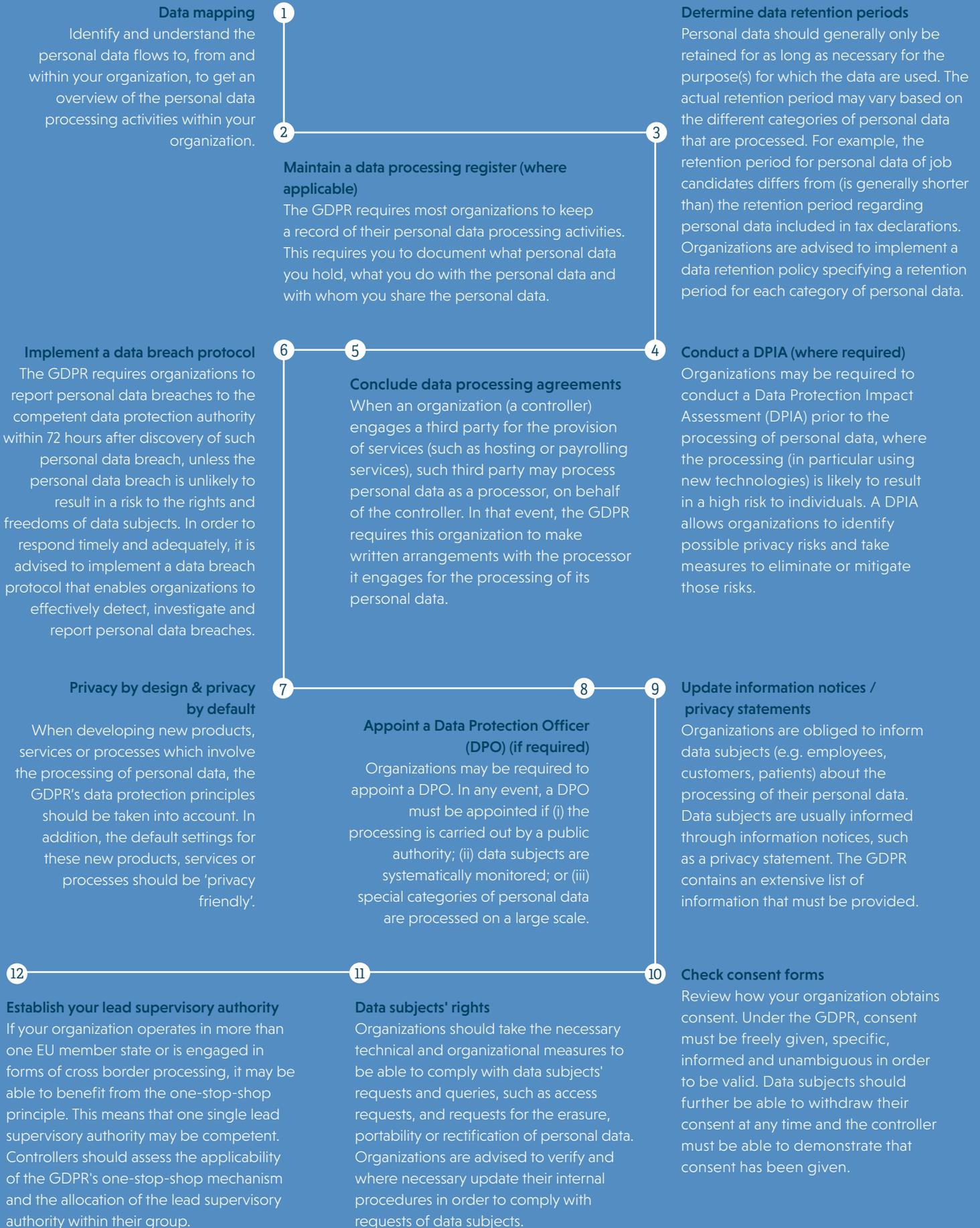
Technical and organizational measures shall be taken to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage.

## ACCOUNTABILITY

The controller is responsible for, and must be able to demonstrate compliance with, the above data processing principles. This means that organizations are expected to implement technical and organizational 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 organizations should comply with its principles. We advise organizations to take the following steps towards compliance with the GDPR.





## 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

This publication serves as a general overview of the GDPR's (potential) impact on your business. Houthoff is an independent law firm that supports clients with highly specialized legal and market expertise. The information set out herein derives from public and/or third party sources. Houthoff shall not be liable for any error in or omission from this information, nor for the use by any party of this information. A recipient hereof must make himself/herself aware of, and comply with, any local laws before using or distributing any of this information.

[www.houthoff.com](http://www.houthoff.com)