

NEW & UPDATED  
(2019)

# THE NEW EU DATA PROTECTION RULES

A GUIDE FOR RETAILERS



This guide, updated to take account of latest guidance produced by data protection authorities and other developments, was written by Joanna Lopatowska, head of consumer and e-commerce policy at EuroCommerce. It provides an outline of the provisions of the EU General Data Protection Regulation 2016, and gives informal guidance on the issues which retailers needed to address ahead and from May 2018, when it came into force.

# Foreword

This guide offers an enhanced analysis and basic information about the 2016 General Data Protection Regulation, and aims to provide some help to retailers in how to comply with the Regulation. I am greatly indebted to my colleague Joanna Lopatowska who undertook the major task of significantly updating and improving the guide she wrote two years ago. This new and updated version benefits from her learnings and insights in the implementation of the Regulation by our members, and the conversations she had with data protection authorities.

Personal data is a major and valuable asset for retailers in ensuring that they give the best service possible to consumers, in building customer loyalty and attracting new business. The interconnected world in which we live enables sophisticated use of data unimaginable only ten years ago. In equal measure, the dangers of data being compromised, either by intentional attacks or by inadvertent actions by employees or contractors, have also grown exponentially. The volume of personal data held on companies' databases, and privacy issues involved, has led to growing regulatory action at national and EU level, with penalties for breaching the regulations also becoming a major business risk. The EU Regulation imposes a number of additional obligations, but also brings some clarity and more uniform provisions in this important area.

It is said that knowledge is the best defence. This guide cannot be a substitute for professional advice, but we hope that its readers will find it useful in raising the right questions for them to ask, and some pointers towards actions that they need to take under the new Regulation.



**Christian Verschueren**  
*Director-General*



# Abbreviations and symbols used in this guide

---

## EU

European Union

The GDPR is applicable in the European Economic Area (EEA), which comprises of the 28 Member States of the EU, and Iceland, Lichtenstein, and Norway.

## GDPR or Regulation

General Data Protection Regulation 2016/679 of 27 April 2016 – available [here](#) in all EU languages.

*GDPR consists of:*

- > 99 Articles, which set out legal rules
- > 173 Recitals, which set out interpretative rules and examples

## DPA

Data Protection Authority / Supervisory Authority

Each Member State designates one or more independent public authorities to enforce the GDPR

- > EDPB (European Data Protection Board) – A formal legal body comprised of the heads of one supervisory authority of each Member State (under the GDPR)
- > WP29 (Article 29 Working Party) – An informal network of the data protection authorities (the Data Protection Directive 1995/46) – no longer in operation

Guidelines and opinions from the EDPB and WP29 are mentioned in this guide in a box

*Guidelines from the Article 29 Working Party*

***Guidelines on transparency under Regulation 2016/679, WP 260, rev.01, last revised on 5 April 2017***

## DPO

Data Protection Officer



*Comments and examples on specific rules and requirements (in italic and blue).*

## DISCLAIMER

The purpose of this guide is to provide basic information about the General Data Protection Regulation (GDPR), to promote compliance, and to help retailers in the transition to the new regime. This guide in no way replaces legal advice. EuroCommerce takes no liability for any measures companies take to implement the GDPR. If companies have any legal questions or concerns, they should seek professional legal advice. This document is for EuroCommerce members only. Reproduction and/or distribution is not allowed without the express consent of EuroCommerce. Quotations are authorised, provided the source is acknowledged.

# Contents

Executive Summary .....	9
What is the GDPR and why is it relevant for retailers? .....	13
.....	
<b>1. GETTING FAMILIAR WITH DATA PROTECTION .....</b>	<b>15</b>
1.1. When and why retailers use personal data? .....	15
1.2. Examples of personal data typically processed by retailers .....	16
1.3. Personal data and other key concepts .....	17
1.4. Which companies must comply with the GDPR? .....	20
1.5. Overview of current EU data protection laws .....	24
.....	
<b>2. GENERAL RULES .....</b>	<b>27</b>
2.1. Data protection principles .....	27
2.2. Legal basis. When can companies process personal data? .....	30
.....	
<b>3. CUSTOMER PRIVACY IN THE RETAIL CONTEXT .....</b>	<b>39</b>
3.1. Selected consumer privacy issues relevant for retailers .....	39
.....	
<b>4. INDIVIDUALS' RIGHTS .....</b>	<b>47</b>
4.1. Key individuals' rights concerning their personal data .....	47
4.2. Redress and legal claims .....	58
.....	
<b>5. ACCOUNTABILITY .....</b>	<b>63</b>
5.1. Key accountability requirements .....	63

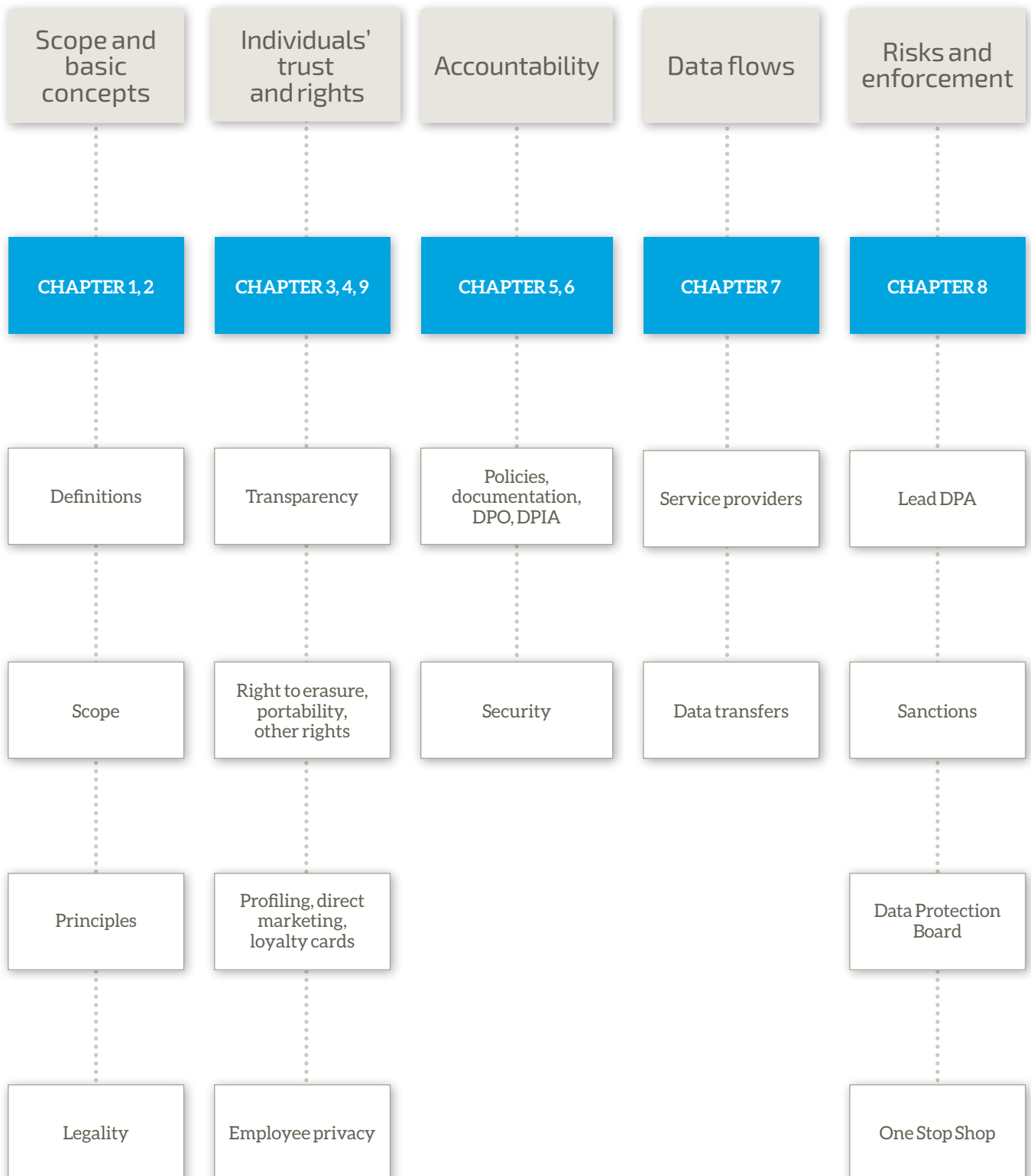
<b>6. DATA SECURITY</b>	75
6.1. Basic information about data security	75
6.2. Personal data breaches	79
<b>7. DATA FLOWS</b>	87
7.1. Data controllers and data processors	87
7.2. Engaging service providers	89
7.3. Basic principles on transferring personal data outside the EEA	91
<b>8. ENFORCEMENT</b>	97
8.1. Data Protection Authorities (DPAs) and One-Stop-Shop	97
8.2. Sanctions	101
<b>9. PRIVACY IN THE WORKPLACE</b>	107
9.1. Privacy in the workplace	107
<b>10. ADDITIONAL INFORMATION</b>	113
10.1. Data Protection Checklist	113
10.2. GDPR guidelines from Data Protection Authorities	116





# Executive Summary

---



## 1. Getting familiar with data protection

Companies should get to know, and be comfortable with, general data protection concepts and understand their primary responsibility for the fairness, legality and security of the processing of personal data.

This affects both big and small retailers, selling on- line and offline. A data protection reflex should become an integral part of each company's way of operating.

Many of the Regulation's main concepts and principles are the same as those in the Data Protection Directive. Therefore, if a company complies with the current obligations, the general approach to compliance and the way of doing things will remain valid under the GDPR.

However, there are new elements. Therefore, companies will have to do certain things for the first time and certain others differently.

## 2. Principles and legality

Companies should ensure that they are transparent about their use of personal data and the reasons for doing so. If a retailer collects personal data, it should have a relevant privacy notice in place.

Companies that already provide privacy notices should update them by adding any missing details. Privacy policies should be robust and clear, be available on the website and be regularly updated.

Companies should identify all the legal reasons for which they process personal data. Companies will have to explain these in the privacy notice.

## 3. Customer privacy in the retail context

The GDPR does not provide for any specific rules on the processing of personal data in the retail context.

There are, and there will be, many questions on how the GDPR applies to the retail sector, which practices are permitted and may continue, and where retailers will need to change the way they handle personal data.

Under the GDPR, retailers will need to explain, in a much clearer and accessible way, how they and their business partners process customer data.

## 4. Individuals' rights

In addition to existing rights to access, rectification and deletion, individuals have new rights they can exercise, such as the right to data portability, and the right to erasure.

Companies should have procedures in place to handle individuals' requests in these areas.

## 5. Accountability

Companies should integrate privacy accountability in all their strategies and projects involving personal data.

Companies should have appropriate policies in place to ensure and demonstrate compliance. These policies should be regularly reviewed to make sure they are up-to-date.

Each company should develop a privacy culture and train staff to understand and fulfil their obligations. Privacy awareness should be raised internally.

As part of building privacy accountability, companies should audit what personal data they collect, from whom, for which purposes and with whom they share the data.

Companies should document their data processing operations and keep the documentation up-to-date. Where required or practicable, companies should appoint a Data Protection Officer (DPO) to take responsibility for data protection compliance.

Accountability also requires creating procedures for data privacy impact assessment (DPIA) to review any risky processing and steps to address the concerns.

## 6. Data security

Companies should have robust security policies and standards in place and fix any security gaps.

There should be a data breach response plan to detect, investigate and report a personal data breach. Employees should be trained to understand their data security obligations so that they know how to prevent breaches and what to do in case of a breach.

## 7. Outsourcing and offshoring

Companies should review contracts with service providers and determine if additional agreements or changes are needed in light of the new requirements.

Companies transferring personal data outside the EEA should ensure that they have appropriate safeguards to do so legally. These safeguards could be either transferring personal data to adequate (safe) countries or using contracts (Standard Contractual Clauses), Binding Corporate Rules (BCRs), or individuals' consent. Transferring personal data to the U.S. could also be based on the Privacy Shield Agreement.

## 8. Enforcement

New enforcement rules are much more stringent, and penalties are significantly higher, compared to the existing rules. Companies that do not comply with the new rules will be exposed to increased enforcement risks.

Companies should identify which data protection authority (DPA) they come under. The lead DPA is determined according to where the company has its main administration or where decisions about data processing are made.

## 9. Privacy in the workplace

GDPR compliance is not limited to customer data. Each retailer, acting as an employer, has privacy obligations towards its employees. As employment laws differ across the EU the GDPR leaves it up to the Member States to adopt specific rules on privacy in the workplace, covering issues like recruitment, performance of the employment contract, health and safety, etc. Companies need to comply with the relevant national laws in this regard. However there are also some common principles on transparency, legal basis and monitoring at work developed by the data protection authorities.

## 10. Checklist

Companies can use the checklist at the end of this guide as a tool to help them implement key privacy compliance requirements and new obligations under the GDPR.

The checklist is not comprehensive. Each company will need to tailor the measures it needs to take, depending on the risks involved in data processing, categories of personal data processed and purposes for which the data are processed. Companies should seek legal advice where any questions arise.



# What is the GDPR and why is it relevant for retailers?

All retailers, whether big or small, selling online or face-to-face, need to know their customers. For that reason, they need at least some of their customers' personal data. Indeed, every day, customers provide retailers with personal data. Retailers use that data for many purposes: customers' address to ship them goods, online browsing history or loyalty card details to better reach the customers, etc.

A retailer may collect and use personal data for various purposes, but at the same time is responsible for using that data in a transparent, legal and secure way.

***The General Data Protection Regulation (EU) 2016/679 of 27 April 2016 ("Regulation" or "GDPR") regulates the rights of individuals over their personal data and the obligations that companies must comply with when using that data.***

The Regulation builds on existing rules under the Data Protection Directive 95/46/EC (the "Directive") from 1995.

The last 20 years have brought enormous changes in technology, data systems and the way people use and share information about themselves. The GDPR updates the existing rules to suit modern life and harmonises them across the EU.

People are more aware - and concerned - about what happens with their personal data, who has access to that data and whether it is secure. Therefore, retailers need to work on building and maintaining customer trust, and proving that they are able to ensure the security of personal data.

The Regulation sets out changes to the rules applicable to almost every area of the processing of personal data. There are also new standards of compliance. Companies will face additional administrative burdens and liability for violations will increase, as will the likelihood of enforcement action.

Implementing the GDPR will certainly require many internal changes. Planning for these will be helpful in making the right decisions.

If, hitherto, companies have not implemented robust privacy standards, they will have to do so under the GDPR. This may require additional resources and different approaches.

In this guide, we outline some of the key areas in which the retailers operating in the EU will be impacted. It does not cover all the provisions of the GDPR. This guide in ten chapters presents selected key data protection issues that companies may wish to consider.

## KEY CHANGES

### HARMONISED RULES

The same rules will apply across the EU in most areas

### RISK BASED APPROACH

Companies have different obligations depending on the risks involved in data processing

### NEW OBLIGATIONS FOR COMPANIES

Records of data processing and policies, security (breach notification), Data Protection Officer (DPO), Privacy Impact Assessment (PIA), Privacy by design and by default

### NEW AND STRONGER RIGHTS FOR INDIVIDUALS

Transparency, data portability, data erasure

### DATA FLOWS

Prescriptive contracts with service providers

### HIGH FINES FOR VIOLATIONS

Sanctions up to 20 million EUR or 4% of global annual turnover

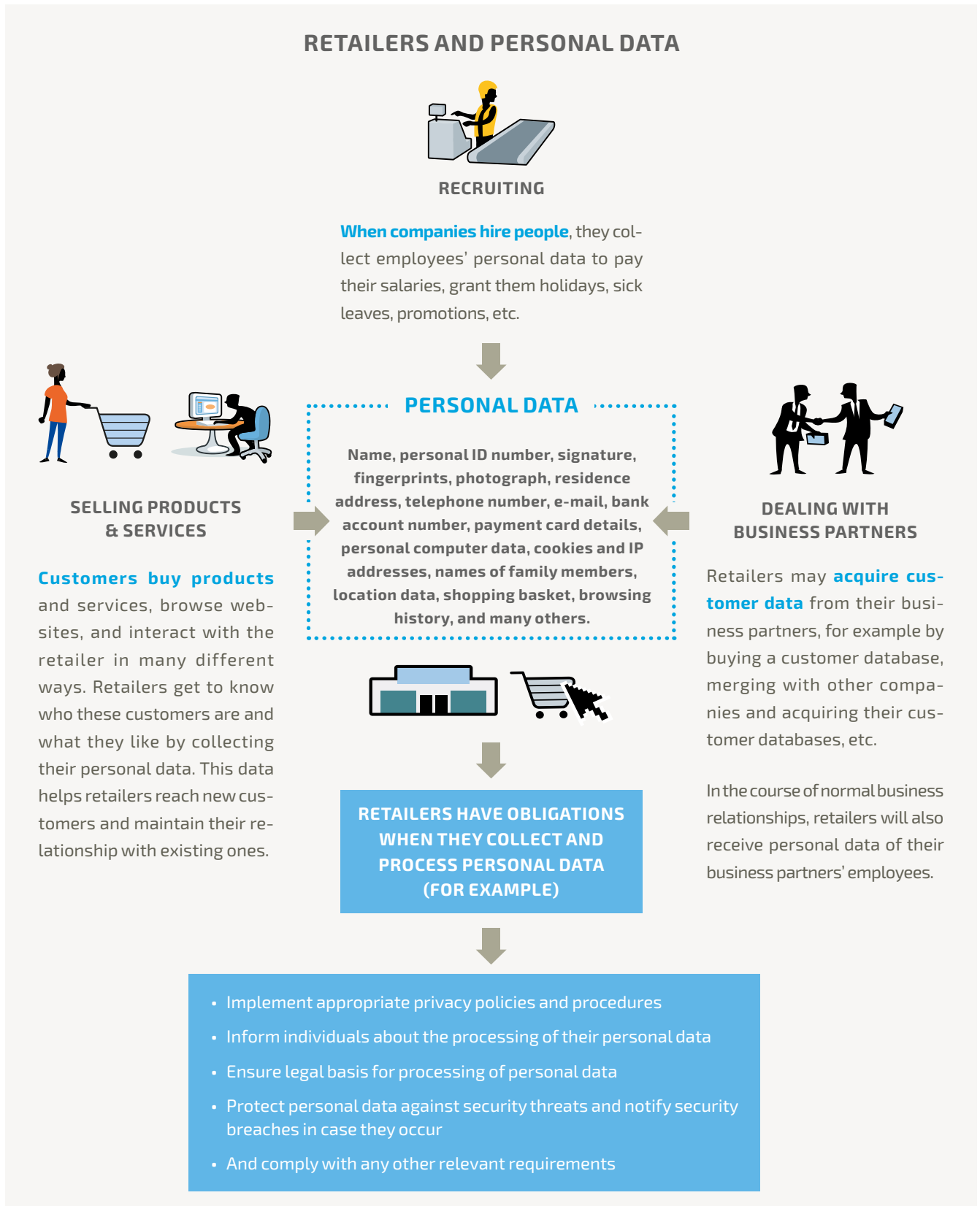


## CHAPTER 1

# Getting familiar with data protection

In this chapter: Retailers and personal data • Definitions • Overview of EU privacy laws • Scope

### 1.1. When and why retailers use personal data?



## 1.2. Examples of personal data typically processed by retailers

### Customer personal data

**Personal details:** name, email address, phone number, other contact details, Facebook or Twitter account, work or home address.

**Purchase data:** goods or services ordered or requested, payment and credit history details.

**Support inquiries:** telephone numbers and duration of any calls requesting support, content of support queries and/or complaints.

**Online information:** online identifiers, including IP addresses, user name and password, user preferences, information gathered through cookies and other web tracking technologies, including content, mailing lists for which the individual has opted-in, location data.

**Other data:** customer's car licence plate, customer's shoe and clothes' size, social network account and activity.

### Employee personal data

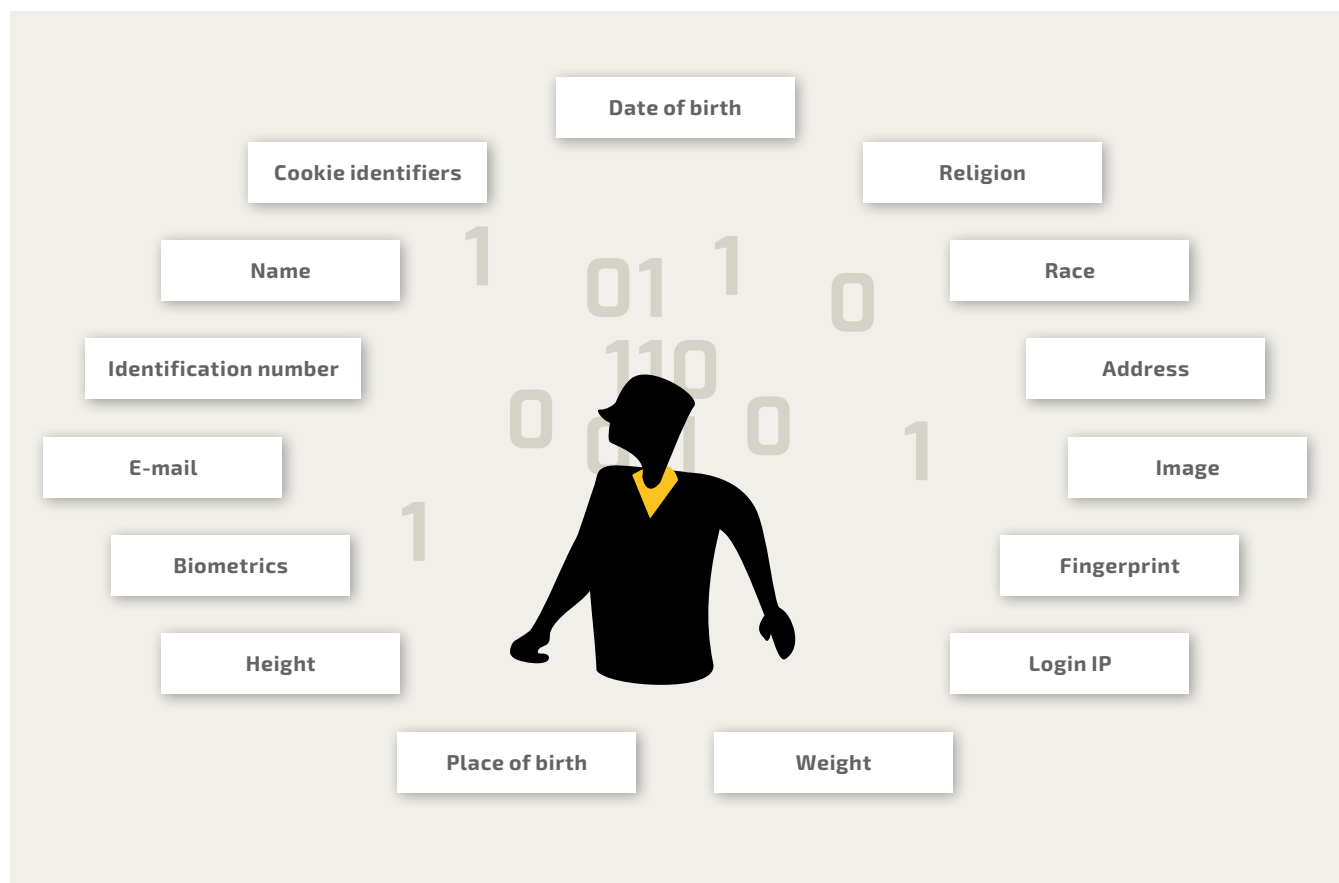
**Personal details:** name, contact details (email, phone numbers, address), gender, date and place of birth, marital status, dependants, emergency contact information, photograph.

**Official identifiers:** citizenship, national ID number, social security number, passport data.

**Salary:** base salary, bonus, benefits, compensation type, salary reviews, banking details, working time records (including vacation and other absence records).

**Position:** description of a position, job title and function(s), employment status and type, branch/ unit/department, full-time/part-time, terms of employment, work history, hire and termination date(s) and reason, length of employment, retirement eligibility, promotions and disciplinary records.

**Talent management:** details contained in letters of application and résumé/CV (previous employment, education history, professional qualifications, language and other relevant skills, certification), skills and experience, development programmes, performance and development reviews.



Source: Medium, [here](#)



## 1.3. Personal data and other key concepts

### ARTICLE 4 OF THE GDPR

***In order to comply with their obligations under the GDPR, companies should understand basic concepts, such as personal data or processing of personal data.***

#### Personal data

Any information relating to an identified or identifiable natural person - "data subject". An identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The GDPR applies to personal data. It does not apply to data that does not relate to an identified or identifiable natural person or to anonymous data. The GDPR does not apply to companies or deceased persons.

For simplicity, in this guide we have replaced the term "data subject" with "individual."



*Often, a single piece of information such as gender or postal code is insufficient to identify an individual. However, such information in combination with other data can. With the development of the computing technologies, less and less information is needed to identify an individual. Therefore, data that may appear not to be personal at a first sight may turn out to be personal data.*

#### Data controller

The individual or organisation, public or private, agency or any other body, which alone, or jointly with others, determines the purposes and means of processing of personal data.

In this guide we often replace "data controller" with "company".



*A retailer is always a data controller for employees' and customers' personal data. This means that a retailer is primarily responsible for handling personal data in an appropriate way and ensuring the data are processed fairly and securely.*

#### Processing

Any operation concerning personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.



*Data processing in the retail context can often include operations, such as:*

- *Asking customers to fill in a form for a loyalty card and using their shopping history data to better target offers.*
- *Analysing customers' shopping preferences via their use of loyalty cards.*
- *Asking customers to provide their address in order to deliver goods bought online.*
- *Holding a contest or a prize draw and asking customers to provide information about themselves.*
- *Tracking customers online and collecting information about their browsing patterns, shopping preferences, and history.*
- *Installing a security camera in a shop and collecting customers' and employees' images.*
- *Using shopping apps on mobile devices to collect information about customers' shopping preferences, tracking their in-store movements.*
- *Keeping records of consumer complaints and requests, including via phone calls.*
- *Sending direct marketing communication.*
- *Collecting contact details to send catalogues, offers, promotions and other marketing materials.*
- *Paying salaries to employees and granting all their employee rights.*

#### Data processor

A natural or legal person, public authority, agency or any other body, which processes personal data on behalf of the data controller.



*A data processor can be:*

- *A payroll provider*
- *Payment service provider*
- *Accountant*
- *Mail marketing provider*

## Data Protection Authority (DPA)

A national supervisory data protection authority is an independent authority tasked with supervising and enforcing data protection rules.

- **Article 29 Working Party (WP29)** – was an advisory body made up of representatives from the data protection authority of each EU Member State, the EU Data Protection Supervisor, and the European Commission.

It was established under Article 29 of the Data Protection Directive 1995/46, and launched in 1996.

WP29 has issued many privacy guidelines and opinions. The GDPR has transformed the WP29 into the European Data Protection Board.

- **European Data Protection Board (EDPB)** – is a transformed WP29 with similar membership composed of the representatives from the data protection authority of each EU Member State.

The EDPB is an EU body with legal personality and extensive powers to solve disputes between national DPAs, to give advice and guidance, and to approve EU codes and certification.

## Consent

Any freely given, specific, informed and unambiguous indication of his or her wishes by which the individual (data subject), either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.



*A pre-ticked box in an online form is not a valid consent. Requesting consent for direct marketing bundled with acceptance of terms and conditions is not appropriate as such consent is not freely given.*

## Profiling

Any form of automated processing of personal data involving using those 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.



*Retailers collect vast amounts of data about sales, consumption, customer shopping patterns and preferences, distribution, and related services. IT technology provides tools to collect and analyse such data in order to reach consumers more effectively by providing targeted offers. Profiling can be done, for example by tracking consumer behaviour on a website, via a shopping app, tracking consumer location, analysing browsing and shopping history. Profiling helps identify customer buying patterns and behaviours, improve service for better customer satisfaction retention.*

## Pseudonymous data

The processing of personal data in such a way that the data can no longer be attributed to a specific individual (data subject) without the use of additional information as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.



*Pseudonymous data does not directly disclose an individual's identity, but it may still identify an individual by associating him with additional information. In other words, pseudonymisation means replacing any identifying data with a pseudonym (a number, letter, other value) which does not allow the individual to be directly identified. Pseudonymous data remains personal data: therefore, many obligations in the Regulation apply. But there are some exemptions and the rules affecting pseudonymous data are less stringent. For example, profiling based exclusively on pseudonymous data is not perceived as significantly affecting individuals.*

## Anonymous data

The term is not defined in the GDPR. Data can be considered anonymised when it does not allow identification of the individual and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information. Data which has been irreversibly anonymised ceases to be personal data, and so it can be used without having to comply with the GDPR.



*In some cases, it is not possible to effectively anonymise data, either because of the nature or context of the data, or because of the use for which the data is collected and retained. The computing technology developments make it increasingly difficult to irreversibly anonymise data.*

## **Enterprise**

Any natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

### **Main establishment**

This is a place where the central administration of a data controller is located in the EEA, unless another entity located in the EEA takes decisions about the purposes and means of the processing of personal data and this entity has the power to implement such decisions.



*A main establishment will usually be the company's headquarters.*

### **Special categories of (sensitive) data**

Any data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data, or data concerning health or sex life or sexual orientation. Data on criminal offences and convictions is not formally regarded as sensitive. However, there are restrictions on the processing of such data.



*In a typical scenario, retailers usually do not collect any sensitive data on their customers. Retailers may collect some sensitive data on their employees, for example, concerning health or trade union membership. Retailers may also be using biometric data, for example for managing employee working time, allowing access to secure areas.*

## **Health data**

Personal data related to the physical or mental health of an individual, including the provision of healthcare services, which reveal information about his or her state of health.

### **Biometric data**

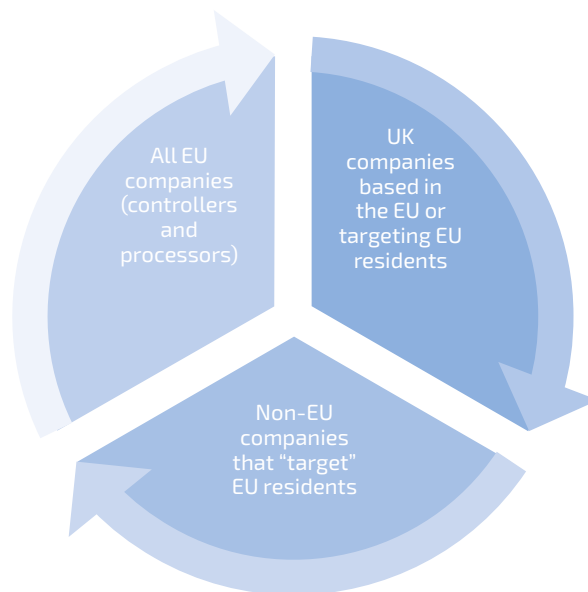
Any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that individual, such as facial images, or "dactyloscopic" (fingerprint) data.

## **Genetic data**

All personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question.

## 1.4. Which companies must comply with the GDPR?

### ARTICLE 3 OF THE GDPR



***All companies established in the EU, whether big or small, selling online or face-to-face, must comply with the GDPR. Some non-EU based companies that do business in the EU are also covered and must comply with the Regulation's obligations.***

#### ***Application of the GDPR to companies established in the EU***

The GDPR applies in the 31 Member States of the European Economic Area (EEA), which includes:

- 28 Member States of the European Union (EU),
- Norway, Liechtenstein and Iceland.

Any further reference in this guide to the EU covers EEA.

According to the GDPR any company (data controller and data processor) established in the EU must comply with the GDPR irrespective of where the personal data is located or where the processing takes place.

The Regulation also applies if the EU-based company stores or manages personal data outside the EU, for example, where personal data is hosted on servers in India or stored in the cloud in the U.S.

#### ***Application of the GDPR to companies established outside the EU***

Many online businesses from outside the EU make their websites available in the EU and target individuals in the EU. These are covered by the Regulation. Targeting individuals means for example, having website or advertisements in a language used by residents of certain countries with the possibility of ordering goods and services in that language, or accepting local currency (Recital 23).

The GDPR applies to any company (data controller or data processor) established outside the EU, if that company essentially targets EU residents. This means, the company:

- Offers goods or services to EU residents; or
- Monitors the behaviour of EU residents (such as profiling or tracking them online).



***For example, a U.S. retail chain that markets its products directly to EU residents, but has no physical presence in the EU needs to comply with the GDPR. A company whose website is accessible to EU consumers will not automatically be covered by the Regulation if it is not actively targeting Europeans.***



***Any company established in the EU and operating a bricks & mortar shop, selling goods online, or operating an omni-channel business will need to comply with the GDPR.***

## ***The impact of Brexit on the application of the GDPR***

Until the end of the planned transition period, and the UK's effective exit, EU law including the GDPR, will continue to apply in the UK.

The relationship between the UK and the EU after Brexit is still uncertain. When a final agreement is reached, the UK will become a "third country" under the GDPR. The GDPR will still be applicable to those UK businesses that:

Have an establishment in the EU;

Process personal data to offer goods or services or monitor behaviour in the EU.

For other companies in the UK, the rules on personal data transfers outside the EU will apply. This means data transfers will be possible, based on:

- Appropriate safeguards, such as standard contractual clauses, Binding Corporate Rules, code of conduct and certification mechanisms.
- Adequacy decision issued by the European Commission concerning the UK.

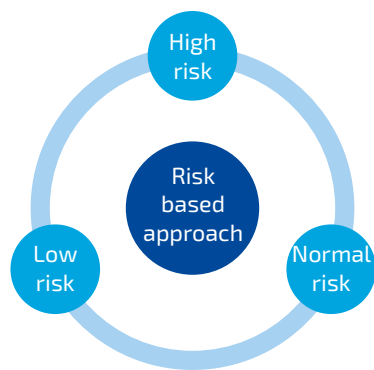
After Brexit, the UK will not be subject to the decisions of the European Data Protection Board. This may lead to divergence between the interpretations of the GDPR developed by European Data Protection Board and those by the UK Information Commissioner's Office (ICO), the UK data protection authority.

The UK ICO will no longer participate in the European Data Protection Board, thereby losing its influence on the decisions and interpretation of the GDPR.

For more information see:

***European Commission Notice to stakeholders on Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection, available [here](#).***

## Does the size of a company matter for compliance with the GDPR?



The GDPR sets out rules that all companies operating in the EU must follow, irrespective of their size, turnover and business model.

**In general the size of a company does not matter. What matters are the risks that a company undertakes when processing personal data.**

The GDPR is built on a so-called “risk based approach”. It means that companies should implement privacy measures corresponding to the level of risk of their data processing activities. The GDPR does not explain on how companies should assess and quantify risk.

Generally, there are three categories of risk:

### High risk

This includes: systematic and extensive automated profiling, large-scale processing of special categories of data, large-scale, systematic monitoring of a publicly accessible area.

Companies have higher requirements, for example, they may be required to perform a privacy impact assessment, consult with a DPA, and, in the case of a data breach, it may need to notify the affected individuals.

According to Recital 75, processing which could lead to physical, material, or non-material damage would be particularly likely to constitute ‘risky’ processing requiring particular attention. Recital 75 further provides the following examples as potentially risky processing, including:

- Processing that may give rise to discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;

- Processing that might deprive individuals of their rights and freedoms or prevent them from exercising control over their personal data;
- Processing of sensitive personal data or data relating to criminal convictions or offences;
- Processing for purposes of profiling;
- Processing of personal data of vulnerable natural persons, in particular of children; and
- Processing involving a large amount of personal data and affecting a large number of individuals.

### Normal risk

For processing operations that do not involve high risks, companies must adopt compliance measures that are appropriate to the risk level of their activities. These measures are not specified in a prescriptive way.

### Low risk

Low-risks data processing activities have not been defined. They are subject to case-by-case analysis. Where the risk is low, a company may be exempt from some obligations, for example to notify the DPA about a data breach.

In general, small retailers will bear low risks.

- For such small companies, the GDPR also provides some relief from the compliance obligations. For example, companies with less than 250 employees are exempt from the record-keeping (documentation) obligation (Article 30.5). However, it is recommended that each company establishes such a record to be able to understand and monitor what personal data it processes, for which purposes and with whom it shares the data.

*In practice, large retailers will need to undertake different compliance measures compared to smaller shops. Such measures will also be different for companies selling on-line (usually collecting large amount of personal data) and bricks and mortar shops (often collecting only a minimal amount of personal data).*

## Suggested steps for basic GDPR compliance by retailers small and large

SUGGESTED COMPLIANCE STEPS	SMALL RETAILER	BIG RETAILER
<b>Audit</b> systems to identify what personal data are being collected and where they are kept.	Yes	Yes
<b>Data records.</b> Create or update existing database inventory (records of processing).	Not required but recommended	Yes
<b>Accountability</b>	Yes	Yes
<b>Privacy by design</b>	Yes, but to a limited extent in practice	Yes
<b>Data Retention</b>	Yes	Yes
<b>Appoint a DPO</b>	Not likely necessary	Yes
<b>Create Privacy Impact Assessment procedures</b>	Not likely necessary	Yes
<b>Security.</b> Ensure appropriate data security and create a data breach response plan	Yes	Yes
<b>Transparency.</b> Review and revise all privacy notices to employees and customers. Draft new ones if there are none.	Yes	Yes
<b>Rights.</b> Ensure process for exercising individuals' rights.	Yes	Yes
<b>Consent.</b> Ensure existing and new consents are valid, especially for direct marketing and profiling (where needed) and ensure that you are able to demonstrate consent.	Yes	Yes
<b>Outsourcing.</b> Update existing service provider agreements with third parties that process personal data on your behalf	Yes	Yes
<b>Transfer.</b> If you transfer personal data outside the EU, ensure you rely on appropriate safeguards.	Yes	Yes
<b>Training.</b> Organise privacy awareness training for employees	Recommended	Recommended
<b>Other.</b> Take any other relevant privacy measures appropriate to the risks involved in the processing of personal data by your company depending on a number of customers, customer tracking and profiling, data security risks, collection of sensitive data, etc.	Not likely to be necessary	Yes

## 1.5. Overview of current EU data protection laws

LAW	BRIEF DESCRIPTION	HARMONISATION	STATUS
<p><i>General Data Protection Regulation (GDPR)</i></p> <p><i>(EU) 2016 / 679</i></p>	<ul style="list-style-type: none"> <li>Horizontal rules regulating the processing of personal data in all general aspects of privacy such as principles, collection and use of personal data, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Full</li> <li>Member States will keep competence to adopt data protection rules in some areas.</li> <li>Direct effect – no need for national implementation.</li> </ul>	<ul style="list-style-type: none"> <li>Fully applicable as of 25 May 2018.</li> </ul>
<p><i>e-Privacy Directive</i></p> <p><i>2002 / 58 / EC</i></p>	<ul style="list-style-type: none"> <li>Regulates privacy in electronic communication such as cookies, unsolicited communication.</li> </ul>	<ul style="list-style-type: none"> <li>Minimum</li> <li>Implementation and enforcement vary across the EU.</li> </ul>	<ul style="list-style-type: none"> <li>Currently in place but is under legal review.</li> <li>ePrivacy Regulation proposed in 2017 to align the e-Privacy rules with the GDPR.</li> </ul>
<p><i>Network and Information Security NIS (Cybersecurity) Directive</i></p> <p><i>(EU) 2016 / 1148</i></p>	<ul style="list-style-type: none"> <li>Regulates Member States' and some types of companies' cybersecurity obligations.</li> </ul>	<ul style="list-style-type: none"> <li>Minimum</li> <li>The Directive to be implemented in national law by 9 May 2018.</li> <li>Laws will vary across the EEA.</li> </ul>	<ul style="list-style-type: none"> <li>Fully applicable as of 9 May 2018.</li> </ul>



## THIS CHAPTER COVERED



### **Retailers' collection of personal data**

Retailers collect personal data from their customers when they buy products and services, browse websites, and interact with the retailers in many other ways. Collecting customers' personal data helps retailers reach new customers and maintain a relationship with the existing ones. Retailers also collect personal data from their employees. Certain personal data on employees is needed in order to pay their salaries and generally manage their employment relationship.

### **Retailers' obligations**

Retailers have many obligations related to their handling of individuals' personal data, including transparency about the purposes for which they process personal data, obligation to secure the data against accidental or unlawful leak, documentation. Obligations of SME retailers will often differ from the obligations of large retailers.

### **Scope**

Any retailer established in the EEA, or targeting EEA individuals to comply with the GDPR, whether big or small selling online and offline.



## CHAPTER 2

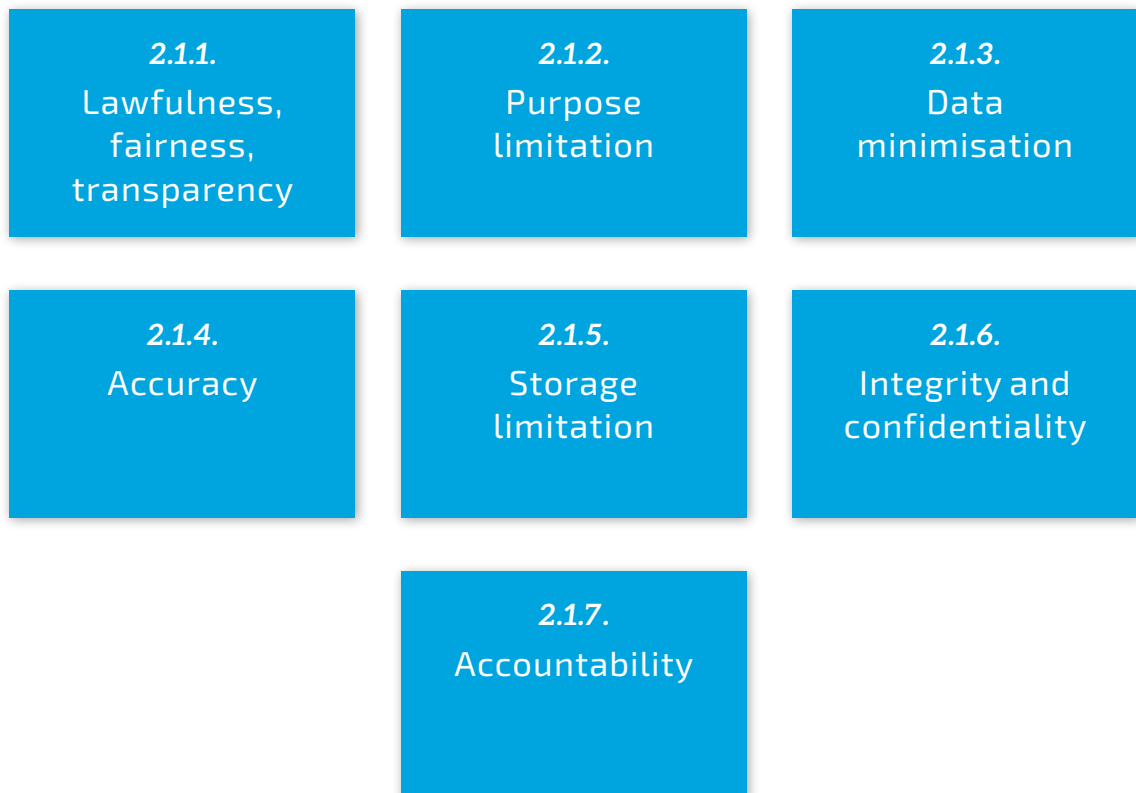
# GENERAL RULES

---

In this chapter: Principles • Legal basis for data processing

### 2.1. Data protection principles

ARTICLE 5 OF THE GDPR



***The data protection principles serve to guide the application and interpretation of the GDPR. Many concepts and rules are designed to take account of further technology developments to avoid the Regulation becoming quickly outdated. The principles aim to adjust the Regulation to changing technology. Therefore the Regulation is technology neutral. It will stay relevant in the future.***

The Regulation builds upon the existing data protection principles, including fairness, lawfulness, transparency, purpose limitation, data minimisation, data quality, security, integrity and confidentiality. A new accountability principle has been added requiring companies to demonstrate privacy compliance.

There are seven principles under the GDPR.

### 2.1.1. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and in a transparent manner. When a company collects personal data it must clearly inform the individual about why that data is being collected and how the data will be used.



*A company must have a lawful reason for processing personal data. For example:*

- **Consent:** an individual has consented to the processing of his or her personal data.
- **Contractual need:** there is a contractual need (selling goods online requires payment and address details to process the order and deliver the good).
- **Legitimate interest:** there is a business need for using personal data (e.g. marketing purposes).
- **Legal obligation:** a company needs to comply with legal obligation (provide information about employees' salaries to tax authorities).

### 2.1.2. Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The purpose must be known to the individuals. It is not possible to simply indicate that personal data will be collected and processed.

Processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which data was collected. Processing for another purpose later on requires further legal permission or consent. The only exception is where the "other purpose" is "compatible" with the original purpose. Indications of this will be any link with the original purpose, the context in which the personal data has been collected, the nature of the personal data, the possible consequences of the intended further processing for individuals, or the existence of appropriate safeguards.



*For example, if a company organises a contest or a promotional activity and collects personal data such as names and email addresses, the company can only use that data for the purposes communicated to the individuals in the context of this promotional activity.*

### 2.1.3. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Companies must be sure that they only keep the minimum amount of data required for their purpose. Each company shall assess how much data is needed and ensure that irrelevant data is not collected.



*Only personal data that are relevant for a particular purpose should be collected. For example, to process an online order, a company will collect payment details, contact and delivery address, etc. Personal data such as age are not necessary to sell goods or ship a parcel, unless for age-restricted goods, such as alcohol or tobacco.*

### 2.1.4. Accuracy

Personal data must be accurate and kept up to date. Companies should take reasonable steps to ensure that personal data that are inaccurate are erased or rectified immediately. They should have a process and policies in place to address how they will maintain the data they are processing and storing.



*For example, a customer database should be updated if there were changes in the shipping addresses, or customers have opted out of email marketing.*

### 2.1.5. Storage limitation

Personal data should be stored for the shortest time possible to permit the identification of individuals. That period should take into account the reasons why the company needs to process the data, as well as any legal obligations to keep the data for a fixed period of time. Each company should establish data retention policies with time limits to erase or review the data stored.



*For example national labour, tax or anti-fraud laws may require companies to keep personal data about employees for a defined period; these limitations will also be governed by e.g. product warranty duration, etc.*

### 2.1.6. Integrity and confidentiality

Personal data must be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.



*Physical, organisational and IT security measures should be in place to protect personal data against theft, misuse or a cyberattack.*

### 2.1.7. Accountability

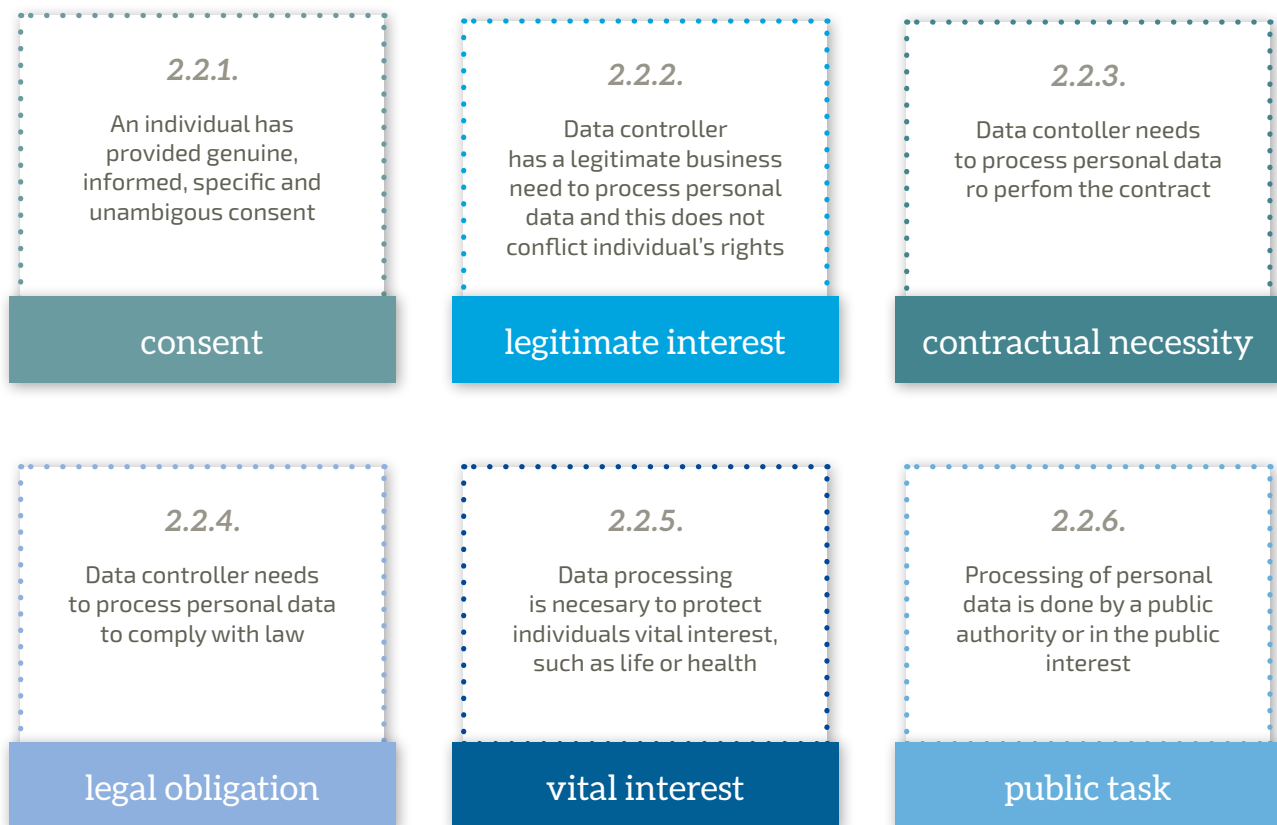
Companies should put in place measures to be able to demonstrate their compliance. They must be able to provide evidence that they have taken the necessary steps to address risks related to processing.



*A company should keep track of what it does with personal data, in particular by keeping an updated inventory of data processing operations.*

## 2.2. Legal basis. When can companies process personal data?

### ARTICLE 6-11 OF THE GDPR



**Companies can process personal data only if they have a valid legal basis – a “good reason” – for doing so.**

There are six available legal bases for data processing. None is better or more important than the other, and relying on a particular legal basis depends on the purpose for the data processing.

Many processes, projects or data processing operations may involve various legal bases at the same time.



*For example, in an employment relationship, the data controller may process personal data of an employee to fulfil an employment contract (contract), pay salaries and grant holidays and sick leave, to comply with the statutory tax and social security obligations (legal necessity), and to manage workforce generally and improve HR processes (legitimate interest).*

However, a data controller can only rely on one legal basis for a particular purpose. If a data controller processes data for multiple purposes, each purpose may have a separate legal basis. For example, if data processing takes place based on consent, Data controller cannot swap between other bases as a back-up if an individual withdraws consent. Controllers have to respect the individual's choice and halt the relevant processing activity.

A legal basis must be established before the data processing begins, and this process should be documented for demonstrating compliance. This is also necessary, as the legal basis must be communicated to the individual in a privacy notice (policy).

In the retail context, the most common legal bases are: **consent, legitimate interest, contractual necessity and legal obligation.**

## 2.2.1. Consent

Consent is one of the fundamental concepts of data protection law in the EU and globally. Consent means that an individual agrees to the collection and the processing of his or her personal data. Consent is seen as the most transparent way to ensure that the data processing is fair and legal. However, the GDPR sets a high standard for consent. Therefore, consent is appropriate if individuals have a real choice and control over how companies use their data.

Despite certain assumptions, consent is not better or more important than other legal bases.

Under the GDPR, consent is defined as **freely given, specific, informed** and **unambiguous** indication of individual's wishes by which the individual, either by a statement or by a clear affirmative action agrees to his or her personal data being processed.

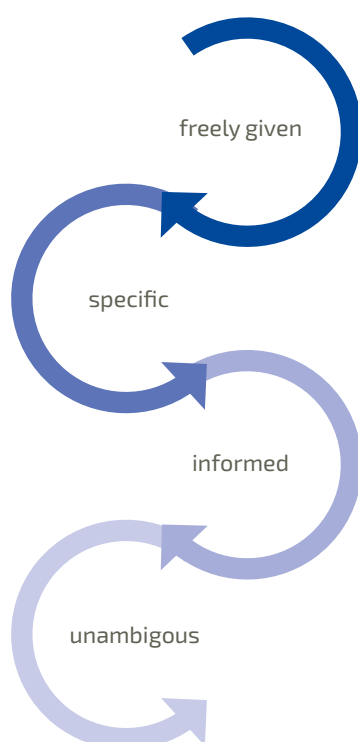
The Article 29 Working Party has issued guidelines on consent. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

**Guidelines on consent under Regulation  
2016/679, WP259 rev.01, Adopted on 28  
November 2017**

**As last Revised and Adopted on 10 April 2018**

### Elements of valid consent



### Freely Given

Freely given means that the individuals have a real choice. For example, performance of a contract or provision of a service must not be made conditional on consent for the processing of data if this is not necessary for the performance of this contract. Consent should not be regarded as freely-given if the individual is unable to refuse or withdraw consent without detriment. It should be just as easy to withdraw consent as to give it. If consent is a precondition of a service, it is unlikely to be the most appropriate lawful basis.

In certain situations, there is no real choice because of an imbalance of power in the relationship with the controller (e.g., between an employer and employee, or citizen and public authority). This means that employers should, by default, avoid seeking consent from their employees

### Specific

Specific means that consent must be separated from any other type of consent and action. According to WP29 guidance, consent should be sufficiently granular, which means that when data processing is done in pursuit of several purposes, the purposes should be separated and separate consent should be contained for each purpose.

For example, a retailer should not use the same consent language to ask its customers for consent to use their data to send marketing emails and to share their details with other companies within their group.

### Informed

Informed consent means that relevant information must be provided in clear and plain language and be distinguishable from other matters (e.g., not hidden in general terms and conditions).

Data controllers relying on consent should carefully review current consent language (in the relevant privacy statement) to ensure the way in which the language is presented and consent obtained meets these enhanced information standards, particularly addressing the individual's right to withdraw consent.

## Unambiguous

Unambiguous means that consent is expressed by a clear action by an individual as opposed to implied or passive behaviour. Pre-ticked boxes are not valid.

According to the GDPR, unambiguous consent may be expressed for example by ticking a box. The WP29 provides an additional range of possible mechanisms to take a clear affirmative action. These could include swiping on a screen, waving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion. All these actions may be valid as long as individuals are clearly informed that the action means consent. Online, consent can be obtained via Internet browser settings, which could mitigate "click fatigue".

## Other requirements for consent

### Demonstrating consent

The data controller must be able to demonstrate that consent was obtained. According to WP29 guidance, data controllers can develop their own mechanisms for documenting consents. However, WP29 suggests to keep a *"record of consent statements received when consent was obtained and the information provided to the data subject."*

In an online context, such records could include *"information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time."*

### Withdrawal of consent

Individuals must be able to withdraw consent as easily as they provided it. According to WP29 guidance, failure to comply with this requirement may invalidate the original consent. "As easily" means that individuals should not have to switch interfaces in order to withdraw consent (e.g., if an individual consents through a website, s/he should not have to email the controller in order to withdraw consent).

If consent is withdrawn, the data controller must cease processing the personal data for the purpose for which consent was obtained, and, if no other basis justifies processing (e.g., data retention), then the controller must delete or anonymise the personal data.

## Children

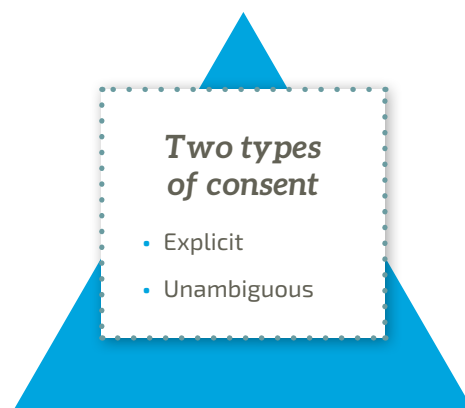
Consent can be confirmed, modified and withdrawn by children once they reach the age of consent. This means that parental consent for the processing of personal data given prior to the age of digital consent will remain a valid ground for processing, providing that the child takes no action upon reaching the age of consent.

### Re-consenting

WP29 states that "if a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must undertake action to comply with these standards, for example by refreshing consent in a GDPR-compliant way".

### Time limits

There is no set time limit for the validity of consent. How long it remains valid depends on the context. However, WP29 recommends that "consent be refreshed at appropriate intervals." There is no further clarification when such a renewal of consent is required, but data controller should not assume that once a consent has been obtained it can be relied on indefinitely.



**Explicit** consent is required for the processing of sensitive data, for profiling and for transfer data outside the EU in absence of other safeguards. Explicit consent must be expressly confirmed in words, rather than by any other positive action. Explicit consent is usually provided in writing.

For other types of processing, **unambiguous consent** will suffice.



## Individual's rights

When the processing takes place based on consent, the individual has:

- The right to withdraw consent. This right needs to be communicated and individuals must have an easy way to opt out.
- The right to data portability, and erasure.



*When relying on consent companies are advised to:*

- **Confirm the legal basis for each purpose of processing personal data and consider using consent only as a legal basis of 'last resort'.**
- **Review the way in which they obtain consent.** If consent is needed for multiple purposes, these will need explaining and addressing separately. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.
- **Review the explanation provided in the consent language.** Consent should be fully informed. This means that information should be provided in a manner people understand. The consent request should be prominent, concise, separate from other terms and conditions, and easy to understand.
- **Implement mechanisms for properly capturing and recording consent and managing the withdrawal of consent.** This is likely to require changes to both the customer relationship and underlying technical solutions used to manage customer preferences.
- **Consent should be obvious and require a positive action to opt in.** Pre-ticked boxes, opt-out boxes or other default settings are not allowed.
- **Consent requests must be prominent, unbundled from other terms and conditions, concise, easy to understand, and user-friendly.**
- **Keep records as evidence of consent – who consented, when, how, and what they were told.**
- **It should be easy for people to withdraw consent at any time they choose.**
- **Keep consents under review and refresh them if anything changes.** Build regular consent reviews into business processes.

## 2.2.2. Legitimate interest

This legal basis allows companies to process personal data without consent when they need to process personal data for their certain interests and these interests are not overridden by the interests or fundamental rights and freedoms of the individuals concerned.

A wide range of interests may be legitimate. These can be either the interests of the data controller or third parties, economic or not.

Legitimate interests is the most flexible lawful basis. However, when assessing whether legitimate interest does not override the individuals' interests or the fundamental rights and freedoms companies need to take into account reasonable expectations of the individuals and whether they can reasonably expect the data processing. Legitimate interest should be avoided if individuals would not likely understand or expect the data processing or if they might object to it. Legitimate interest should also be avoided where the processing could cause harm.

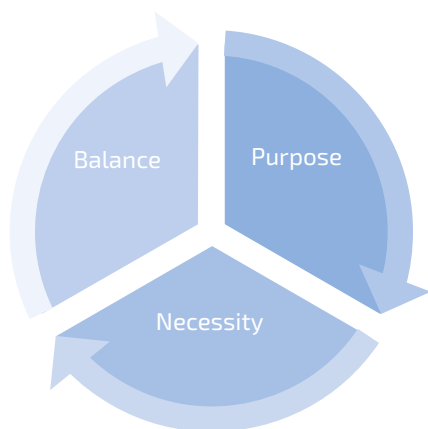
The legitimate interest does not always need to align with the individual's interests. If there is a conflict or impact on individuals, data controller can continue the processing if they can demonstrate the need for it and a compelling benefit for the individual.

### Examples of legitimate interest in the GDPR

- The processing is done in the context of **the client or employee relationship** (Recital 47).
- The processing of personal data is for **direct marketing** purposes. (Recital 47). However, this is limited to postal marketing. Direct marketing via electronic means, such as email, requires consent (under the ePrivacy rules).
- The processing of personal data is strictly necessary for the purposes of **preventing fraud**, for example internal compliance programmes. (Recital 47)
- Personal data is shared with other **affiliated entities in the same group** of companies for internal administrative purposes, including the processing of clients' or employees' personal data. If personal data is transferred outside the EEA, all the restrictions on data transfers apply. (Recital 48). See chapter 7 on data flows.
- The data processing is strictly necessary and proportionate for the purposes of ensuring network and information security (Recital 49)

## Identifying legitimate interest

The data protection authorities (in particular the UK Information Commissioner's Office) recommend to undertake a three-step assessment to identify whether the data controller may rely on the legitimate interest legal basis.



### 1. Purpose test – to identify whether the legitimate interest exists:

- Why does the company need to process the data?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing? How important are they?
- What would the impact be if the processing does not take place?
- Would the processing be unethical or unlawful in any way?

### 2. Necessity test – to identify whether the processing necessary for that purpose:

- Does this processing help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

### 3. Balancing test – to identify whether individual's interests override the legitimate interest:

- What is the nature of the relationship with the individual?
- Is any of the data sensitive or private?
- Would people expect to use their data in this way?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual? How big is the impact?
- Are children's data involved?
- Are any of the individuals vulnerable in any other way?
- Are safeguards possible to minimise the impact?
- Is opt-out possible?

## New purposes

There are some circumstances in which personal data may be processed for new purposes that go beyond the original purpose for which the data was collected (Article 6).

If personal data is to be processed for a new purpose, the company must consider whether the new purpose is "compatible" with the original purpose taking into account the following factors:

- Any link between the original purpose and the new purpose.
- The context in which the personal data has been collected, including the company's relationship with the individual.
- The nature of personal data, in particular, whether sensitive data is involved.
- The possible consequences of the new purpose.
- The existence of appropriate safeguards (e.g., encryption or pseudonymisation).

## Individual's rights

When the processing takes place based on the legitimate interest, the individual has:

- No right to data portability.
- An absolute right to object to direct marketing, which means that direct marketing must stop when someone objects.
- The right to object to other purposes. However, if the data controller demonstrates that the legitimate interests are compelling enough to override the individual's rights the data processing may continue.



*When relying on the legal necessity companies are advised to:*

- *Document the assessment of the use of legitimate interest to be able to demonstrate compliance. There is no standard for such documentation. Keep the record under review and update where there are changes.*
- *Consider referring to the competent DPA if the assessment demonstrates high risks.*
- *Include information that they rely on legitimate interest and explain this interest.*

### 2.2.3. Contractual necessity

The data controller may rely on this legal basis when the processing of personal data is necessary in order to perform a contract. This can take place in two situations:

#### Contract



There is an existing contract with an individual and the data processing is necessary to comply with the data controller's obligations under the contract.



*For example, when buying goods online, the customer needs to provide payment details and delivery address, so that the goods can be paid for and delivered.*



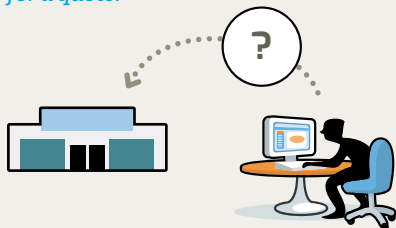
#### No contract



There is no contract, but an individual has requested the data controller to take an action as a first step to concluding a contract.



*For example, an individual requests information from a retailer about a particular product or asks for a quote.*



This legal basis does not apply if the data controller has requested personal data at its own initiative or at the request of a third party.

This legal basis is interpreted very narrowly and only covers those data processing operations which are strictly necessary to perform the contract. However, if the processing is done for some other, broader purposes the data controller will have to consider other legal bases such as legitimate interest or consent.

When selling online, for example, the retailer will need to process the address of the customer in order to deliver the goods. This is necessary to perform the contract. However, profiling of the customer cannot be based on contractual necessity.

#### Individual's rights

When the processing takes place based on the contractual necessity, the individual has:

- No right to object and no right not be subject to a decision based solely on automated processing including profiling.
- The right to data portability.



*When relying on contractual necessity companies are advised to:*

- Document decision which personal data are required for performing the contract.
- Include information about the purposes and which personal data are required to be processed in order to perform the contract.

### 2.2.4. Legal obligation

This legal basis means that the data controller is obliged to process the personal data in order to comply with legal provisions. In most cases it is quite clear from the law that the processing of personal data is necessary for compliance.



*For example, an employer needs to process personal data of the employees in order to comply with the relevant tax and social security obligations.*

#### Individual's rights

When the processing takes place based on the legal obligation, the individual has:

- No right to erasure, right to data portability, or right to object



*When relying on the legal obligation companies are advised to:*

- Identify the legal provision which requires the data processing.
- Document the decision that processing is necessary for compliance with a legal obligation.
- Inform about the legal obligation and the purposes for the processing of personal data in the privacy notice. It is not necessary to cite the relevant law. It might be sufficient to refer to a government website or to industry guidance that explains generally applicable legal obligations.

## OVERVIEW OF THE INDIVIDUAL'S RIGHTS AVAILABLE DEPENDING ON THE LEGAL BASIS

LAW	INFORMATION ACCESS	PORTABILITY	OBJECT	OBJECT TO MARKETING	ERASURE
Consent	✓	✓	Right to withdraw consent	✓	✓
Contract	✓	✓		✓	✓
Legal obligation	✓			✓	✓
Vital interest	✓			✓	✓
Public task	✓		✓	✓	
Legitimate interest	✓		✓	✓	✓

## THIS CHAPTER COVERED



### Principles

The data protection principles serve to guide the application and interpretation of the GDPR. The principles in the GDPR include fairness, lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

### Privacy Notice

Every company must provide a privacy notice explaining in detail for which purposes it collects and processes personal data, who receives the data, etc. A good privacy notice can help reassure customers that a company is transparent and accountable, and that they can trust the company with their personal data. Privacy notices have to be clear and easily accessible. Retailers should identify and review all existing privacy notices and policies concerning employees and customers. Notices should be revised to ensure they comply with the new GDPR requirements.

### Legal basis

Every company should identify in which situations it needs to obtain consumer consent (for example, direct marketing by email), where the company will have legitimate interest to process personal data (for example, direct marketing via postal mail), and where contractual necessity will give sufficient legal grounds (for example, shipping goods ordered online). Under the GDPR consent is defined as any freely given, specific, informed and an unambiguous indication of an individual's wishes.



## CHAPTER 3

# CUSTOMER PRIVACY IN THE RETAIL CONTEXT

---

In this chapter: Profiling • Loyalty cards • Direct marketing • Cookies • Children • Contests • CCTV cameras

### 3.1. Selected consumer privacy issues relevant for retailers



*The GDPR does not contain any particular rules on the processing of personal data in a sector-specific context, such as retail. In addition, privacy rules are designed to be technology-neutral. This means that there are no specific rules about using personal data by retailers for their commercial purposes, whether online, offline or omni-channel. There are, and will be, many questions on how the GDPR applies to the retail sector, which practices may continue, and where retailers will need to revise these. Many of these issues are currently unclear.*

In this chapter we outline some areas where retailers should pay particular attention, as their practices might need to undergo significant change.



## Customer profiling

The more retailers know about their existing and prospective customers the better they can reach out to them. Therefore, establishing customer profiles and data analytics can give retailers information they need to generate business, and can play crucial role in the growth of their business.

Customer profiles include extensive data about customers' age, gender, location, spending habits, income, details of purchasing behaviour, such as products each customer buys, when and how, feedback about how customers rate products or services, and much more.

The GDPR defines profiling as 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 person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Profiling is understood very broadly. According to the Article 29 Working Party, classifying individuals based on age, sex and height could be considered profiling.

**The GDPR regards profiling as a risky activity subject to strict conditions (such as the need for a privacy impact assessment). Therefore, compliance with this new regime should become an important part of all retailers' big data strategies.**

The Article 29 Working Party has issued guidelines on profiling and automated decision making. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

***Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251, rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018***

The WP29 distinguishes two aspects of profiling:

- The taking of **significant, solely automated decisions**.
- **General profiling**. The general rules also apply to significant automated decisions.

## Significant Solely Automated Decision Making

Under the GDPR (Article 22), individuals have the right not to be subject to a decision based solely on automated processing (including profiling) if the decision produces:

- Legal effects, or
- Similarly significantly affects the individuals.

WP29 provides clarification as to the application of the provision.

- Solely means that there is no meaningful human involvement in the decision making process.
- Legal effects are those that have an impact on an individual's legal rights such as statutory or contractual rights. For example: an individual being refused entry at a border, being denied a social benefit).
- Similarly significant effects are those that are equivalent or similarly significant to legal effects. The effect must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned. These effects must be more than trivial. For example: automatic refusal of an online credit application or e-recruiting practices without human intervention.

WP29 takes a restrictive approach:



*Individuals do not merely have a right to object to such decisions, but automated decision making is prohibited unless:*

- *It is necessary to enter into, or to perform, a contract with the individual. Necessity is interpreted narrowly.*
- *It is authorised by EU or Member State law; or*
- *It is based on the individual's explicit consent.*



### Profiling and targeted advertising

According to WP29 typically **targeted advertising would not have a significant effect on individuals**.

Thus, such profiling does not automatically require consent.

However, in certain contexts targeted advertising could lead to a legal or significant effect. This would depend on:

- a. the intrusiveness of the profiling;
- b. the expectations and wishes of the individual;
- c. the way the advert is delivered; and
- d. the particular vulnerabilities of the individuals targeted

For example:

- automated decisions include differential pricing preventing an individual obtaining certain goods or
- an individual with financial difficulties being regularly targeted ads for gambling sites.

- **Right to object to profiling.** The GDPR introduces a new right to object to profiling, even when there is no automated decision making. See more in the next chapter on individuals' rights.
- **Purpose limitation.** Profiling may often involve the processing of personal data that was collected for other purposes. In such case, if personal data is further used for profiling this must be compatible with the purposes for which it was collected. Otherwise, if there is a different purpose, individuals' consent may be required.
- **Data minimisation.** Data controllers should clearly explain and justify the data processing concerning profiling. Data controllers should implement retention periods for profiles. Storing data for too long may conflict with the proportionality principle, in particular as opportunities created by profiling may encourage data controller to collect more data and keep it longer.
- **Accuracy.** Data controllers need to have robust measures in place to verify on an ongoing basis that data reused or obtained indirectly is up to date.
- **Rights.** The GDPR introduces stronger rights for individuals. For example, access rights will cover profiling data.
- **Data Protection Impact Assessment (DPIA).** A DPIA will likely be required for various profiling activities. Under the GDPR significant automated decisions are deemed to be high risk processing requiring a DPIA. However, the WP29 interprets this broadly also including decisions not wholly automate or not only having legal or significant effects.

Even if the profiling related to advertising is not a significant automated decision, data controllers must comply with the general rules on profiling under the GDPR.

The ePrivacy Directive (to be replaced by the proposed e-Privacy Regulation) is also relevant as it covers online tracking, which as a rule requires consent.

### Key compliance steps for general profiling

When profiling customers retailers are advised, in particular, to take the following steps to comply with the GDPR:

- **Privacy notice.** Data controllers must provide concise, transparent, intelligible and easily accessible privacy notice. In addition, data controller must inform that profiling takes place and that the individuals have the right to object. This should be presented clearly and separately from other information.
- **Legal basis.** Where the data controller does not rely on consent, it must be able to justify another legal basis. For example, if the controller relies on legitimate interest, it must balance the interest against individuals' rights. If the controller relies on contract, this must be interpreted narrowly. It is not sufficient to mention in the contract (or terms and conditions) that profiling takes place. It is not enough to make it 'necessary' for the performance of the contract.



## Loyalty cards

Many retailers collect customers' personal data on shopping behaviour and preferences via loyalty programmes.

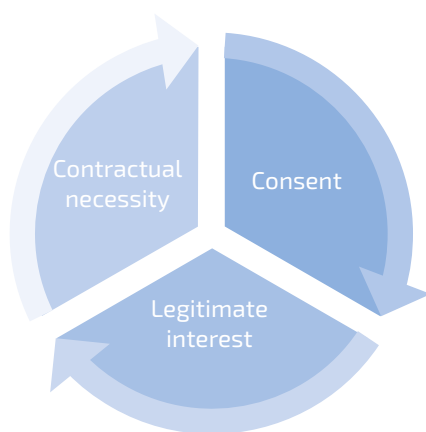
The key issues related to how such loyalty programmes can operate under the GDPR are:

- Whether consent is necessary and the only way to operate such a programme;
- Whether retailers may rely on another legal basis, and if so, for which kinds of operation, and
- Whether loyalty programmes that have been in place before the GDPR became applicable can continue to operate, or whether the retailers should refresh customer consents for these programmes.

**There is as yet no regulatory guidance or formal clarification to these questions. Approaches to the legal basis used for loyalty programmes may differ. Therefore, retailers should pay particular attention to establishing the relevant legal requirements.**

Based on a general reading of the GDPR, retailers operating loyalty programmes may rely on contractual necessity, legitimate interest, or consent. Which legal basis is used will depend on the purposes for which personal data is processed. This means that within one loyalty scheme, one or a combination of the legal bases might be used, each one giving rise to different rights.

This guide should not be taken to provide legal advice in this regard. However, retailers may consider the following.



### Contractual necessity

This legal basis may usually be used merely to establish and manage the customer account, such as to verify the customer's identity and age, allow user settings and similar.

For these purposes, the customer would not have the right to object, but would enjoy other rights under the GDPR.

### Legitimate interest

This legal basis may usually be used by the retailer to develop services or improve products. Collecting personal data from the customer's use of the loyalty programme could allow the retailer to perform analysis on an aggregated level without identifying the individuals or by pseudonymising personal data.

For these purposes, the customer would not have the right to data portability, but would enjoy all the other rights.

### Consent

Consent may be used for a detailed analysis of customer behaviour, such as profiling, and for providing tailored offers and targeted marketing. There could be different types of profiling using different data sets. For example, retailer could analyse browsing patterns, websites visited and specific parts of the website, customer searches, products placed in the basket and products bought, and many others, customer's lifestyle, residential area, interests, and many others.

For these purposes, if the customer has provided consent, he or she would enjoy all the rights under the GDPR.

Retailers need to establish whether old consents obtained from customers before the GDPR became applicable meet the GDPR requirements or whether obtaining new consents is necessary.

Regarding loyalty programmes, the GDPR requires a lot more of retailers if they are to remain compliant. Retailers need to rethink how they use personal data they derive from online shopping and loyalty cards. In particular, any data processing using this information will need to be fully explained to customers in a clear and concise format, with a lot more details than before.

### Key compliance steps

When deploying loyalty programmes, retailers are advised, in particular, to take the following steps to comply with the GDPR:

- **Privacy notice.** Provide a privacy notice providing detailed information, in particular explain legal bases used and inform about profiling and the logic used for this purpose.
- **Legal basis.** Establish which legal basis they rely upon and for which purposes, and clearly inform about it in the privacy notice.
- **Rights.** Provide a process for individuals to exercise their rights to information, access, erasure or objection, and other relevant rights.



## Direct marketing

The GDPR recognises that the processing of personal data for "direct marketing purposes" can be considered a legitimate interest. This means that customer consent will not be required to collect and process personal data for direct marketing purposes. However, this only applies to "traditional" marketing, such as via leaflets or coupons, or catalogues, etc.

Electronic marketing via email or other electronic channels is covered by specific provisions included in the ePrivacy Directive (in 2018 under revision to be transformed into ePrivacy Regulation). These provisions of the ePrivacy Directive (Article 13) generally set out that:

- Consent is required for unsolicited direct electronic marketing
- Those data controllers that have electronic contact details of their customers (obtained in the context of sales of a product or service) may use these contact details for direct marketing of its own similar products or services provided that customers have a clear way to opt out from such messages.

The general GDPR rules on direct marketing is that individuals can at any time object to the processing of their personal data for direct marketing purposes. No justification is needed for such an objection. In such cases, personal data may no longer be processed.

According to WP 29 guidelines on consent, data controllers that process personal data on the basis of consent in compliance with national laws (before the GDPR became effective) are not automatically required to completely refresh all existing consent in order to comply with the GDPR.

Consent which has been obtained to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR.

*This means for example, that data controllers need to be able to demonstrate that valid consent was obtained and have clear records of these consents. This also means that consents need to have been obtained as affirmative actions and not via implied actions or pre-ticked opt-in boxes. Data controllers should also be able to demonstrate sufficient granularity of consent. The individuals should have the possibility to withdraw consent as easily as they have provided consent.*



*If a data controller finds that the consent previously obtained under the old legislation does not meet the GDPR's standards, controllers will need to obtain new GDPR-compliant consent.*



## Children

Children are exposed to privacy risks when their personal data is collected online automatically (e.g. cookies), upon request (e.g. when signing up for a service), or voluntarily, when they fill their personal data in online forms, for example, through surveys, quizzes and contests.

Children often underestimate the value of their personal data and they readily agree to its use in order to access to desired services or websites.

Retailers will collect children's' personal data for certain types of data processing. For example, when rolling out special apps, contests, promotions, and other similar activities directed at children.

The GDPR sets out special rules (Article 8) when:

- Data processing is related to the offer of information society services directly to a child and
- The data processing is based on consent.

When data processing is not based on consent, but on other legal grounds, this provision does not apply.

***The GDPR requires that, for children under 16, parental consent is required. Member States may set a lower age, although not below 13. Children older than 16 may give consent themselves.***

According to the guidelines from Article 29 Working Party:

- Not all information society services are covered, but only these directed to children. When it is clear from the service, or an app that it is directed to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.
- The GDPR does not state any clear requirements to authenticate the age of a child.
- Data controllers are expected to make reasonable efforts to verify that the user is over the age of digital consent. These measures should be proportionate to the nature and risks of the processing activities.
- It is up to the data controller to determine what measures are appropriate in a specific case. In general, data controllers should avoid excessive collection of personal data in order to be able to determine the age (data minimisation). What data is needed to authenticate the age and how the confirmation is obtained depends on the risks inherent in the processing. For example, in low-risk cases, verification of parental responsibility via email may be sufficient. In high-risk cases, it may be appropriate to ask for more proof.

## Key compliance steps

When collecting children's consent, retailers are advised, in particular, to take the following steps to comply with the GDPR:

- Establish whether **it provides information society services** directed to children and whether the GDPR requirements apply.
- If it operates across many Member States, the retailer will need to **establish the rules on the age of consent** in the countries where provides services to children.
- **Provide clear privacy information** that can easily be understood by children.
- Ensure they have a system in place to **verify the age** of the child and that the necessary controls are built in this system.
- Ensure they have measures to **check that someone is the parent or** the guardian of the child that wishes to use your services.
- Ensure they **properly store the parental consent** and make sure it is made available to parents just as easy as the consent was given.



## Prize contests

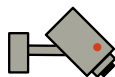
Retailers use prize draws and other such contests and actions in various forms to promote their commercial offers.

Collection of personal data in the frame of such activities is not specifically covered by the GDPR. Therefore, general compliance rules apply.

## Key compliance steps

When undertaking such promotional activities, retailers should, in particular, take the following steps to comply with the GDPR:

- **Privacy notice.** Provide a privacy notice informing participants in a contest about the collection of their personal data via the contest, and for which purposes you will use their data. The policy must be disclosed in an appropriate way to the participants.
- **Data minimisation.** Collect and process only those personal data are necessary for the purpose of the contest and no for other unrelated purposes.
- **Consent.** Establish legal basis for data processing: most likely consent. If you direct contests at children under 16, you will need to obtain parental consent.
- **Rights.** Ensure process for individuals to exercise their rights to information, access, erasure or objection, and other relevant rights.



## Surveillance (CCTV) cameras

Retailers use surveillance cameras for different purposes: to monitor the security of the shop or a warehouse, to prevent theft, to prevent violence and other crime, or to monitor employees.

Images of individuals (even if their faces are not visible), car number plates, or other such information captured on cameras is considered to be personal data.

Therefore, companies operating surveillance cameras in a shop, warehouse, distribution centre, entrance hall, car park, or office space, are processing personal data and therefore must comply with the GDPR.

Retailers setting up cameras are always regarded as data controllers, and they bear responsibility for compliance.

The GDPR does not include any specific rules on the capturing and processing of audio-visual images. This means that the general GDPR rules apply as to any other type of data processing. There are no specific rules about the placing of cameras, information to be provided to people, areas that can be filmed, for how long images can be stored, who has access to images, etc.



*The use of a CCTV camera does not require an individual's consent but companies must ensure privacy safeguards, and in particular inform people of the cameras, ensure data security and allow access to personal data.*

## Key compliance steps

When deploying CCTV cameras, retailers are advised, in particular, to take the following steps to comply with the GDPR:

- **Legal basis.** Justify the reasons for using CCTV – and document them. In almost all cases, data controllers can rely on legitimate interest or the need to comply with legal requirement. However, they will need to ensure that the camera coverage does not violate individuals' rights. This is in particular important in the context of the privacy in the workplace.
- **Privacy Impact Assessment.** As the camera coverage will often involve systematic monitoring of individuals in public spaces on a large scale, they should conduct a Data Protection Impact Assessment (Article 35).
- **Notice.** Inform people that cameras are being used. Display information, including icons or other visuals, which identify who manages the cameras and how to contact the data controller.

- **Retention.** Keep the data only as long as permitted by relevant national laws (for example, in some countries the general rule is that images can be kept for no longer than 30 days) or in the absence of specific laws, as justified. There are no EU-defined acceptable retention times. Each camera and its purpose requires assessment to determine how long footage can be retained. If there is a need to retain CCTV data for longer, then the risk assessment should state how long and why.
- **Rights.** Be able to provide people who have been recorded with copies of their personal data. Ensure that the individual requesting the access to the recordings is present in the footage and that it does not disclose any personal data of another individual. This may involve blurring parts of the footage such as other figures or licence plates.
- **Access to data.** Ensure that third parties with access to CCTV data understand their obligations in relation to GDPR.
- **Security.** Ensure appropriate security measures, regardless of its format, in particular via encryption. Screens displaying live or recorded footage should only be viewed by authorised staff.

Currently some Member States have specific rules on the use of CCTV cameras. In some other countries, DPAs have issued guidance (for example, the UK Information Commissioner (ICO) issued a Code of Practice, available [here](#)). In most countries, general data protection rules apply.



*Here are some tips on what companies may wish to consider when deploying surveillance equipment. These tips are mainly based on the UK ICO guidelines.*

*Companies operating in other member states should check for any relevant laws or guidance.*

- *Cameras should only record what is relevant and when it is relevant.*
- *Cameras should not be placed in places where people have a higher expectation of privacy such as changing rooms or toilets.*
- *Areas under CCTV surveillance should be clearly marked with signs that are clear and prominent, identify the operator of the system, provide contact details, and explain the purpose of the CCTV.*
- *Recordings should be stored in such a way that image quality is preserved and images can easily be extracted from systems when required by law enforcement agencies.*
- *Images must remain secure and only be viewed under restricted conditions with access limited to authorised personnel.*
- *Recordings should be retained for no longer than required for the company's purposes, and only held beyond this if needed by law enforcement agencies.*
- *Disclosure should be limited to circumstances such as preventing or detecting crime or where people ask to view images of themselves.*



## Cookies

Cookies are small files that track users' browsing habits and allow advertisers to target consumers. Cookies and other tracking technologies allow for the collection of personal data. Therefore, they are subject to data protection rules.

Cookies and consumer tracking are subject to two sets of rules:

- **General Data Protection Regulation/GDPR:** Covers general rules on definition of personal data and processing, how can personal data be legally obtained and used, rules on individuals' rights, consumer profiling, consent, etc.
- **e-Privacy Directive:** Covers the transmission of personal data over electronic communications networks. It applies to any information stored on or retrieved from user's device, including cookies and tracking technologies. It is mainly aimed at cookies, but also applies to other technologies (web beacons, advertisement tags).

The ePrivacy Directive is undergoing significant revision, as it is being transformed into a Regulation and aligned with the GDPR. As this legislative work is still in progress, at the time of writing, no detailed analysis is included at this stage.

**Companies should stay on top of the revision of the e-Privacy Directive and any relevant regulatory guidance.**



## THIS CHAPTER COVERED

The GDPR does not contain any specific rules on the processing of personal data in the retail context. There are no specific rules on the use of loyalty cards, collecting children's personal data, operating surveillance cameras or social media activities.

There are some rules on profiling and direct marketing. However, they are quite general.

There are, and there will be, many questions on how the GDPR applies to the retail sector, which practices may continue and where retailers will need to revise these. Many of these issues are currently unclear. What is clear is that, under the GDPR retailers need to explain, in a much clearer and accessible way, how they and their third party partners are using the consumer information they collect. Privacy notices, consent, and legitimate interest are key issues for each retailer.

## CHAPTER 4

# INDIVIDUALS' RIGHTS

In this chapter: Transparency • Individuals' rights • Redress • Legal claims

### 4.1. Key individuals' rights concerning their personal data

ARTICLE 15-22 OF THE GDPR

<p>4.1.1.</p> <p>Provide clear information that you process personal data</p>	<p>4.1.2.</p> <p>Data controller has a legitimate business need to process personal data and this does not conflict individual's rights</p>	<p>4.1.3.</p> <p>Correct inaccurate or incomplete data</p>
Information (Transparency)	Access	Rectification
<p>4.1.4.</p> <p>Delete personal data upon request if data are no longer necessary or an individual has withdrawn consent</p>	<p>4.1.5.</p> <p>Limit the processing if an individual questions the accuracy of data</p>	<p>4.1.6.</p> <p>Allow easy download or moving personal data to another provider</p>
Erasure	Restriction	Portability
<p>4.1.7.</p> <p>Stop processing personal data if an individual objects, in particular to direct marketing</p>	<p>4.1.8.</p> <p>Stop processing personal data if an individual objects to being profiled, unless the individual has consented</p>	<p>4.1.9.</p> <p>Allow an easy way to withdraw consent at any time</p>
Objection	Objection to profiling	Consent withdrawal

***Under the GDPR, all of the existing rights, such as the right to information, correction, or deletion of personal data have been maintained and further reinforced. However, the GDPR has also created new rights, such as the right to be forgotten or right to data portability.***

Companies should have procedures in place to handle requests from individuals within appropriate time. Companies should evaluate whether their IT systems have capabilities to provide information requested by the individuals within a prescribed time.



### 4.1.1. Right to information

**The GDPR requires any company processing personal data to inform individuals about it and provide certain information, such as who the company is and why it collects personal data and may other details. Transparency is a central concept of the GDPR. Ensuring that data processing is clear for consumers is core to building trust with them.**

The **GDPR** sets a high standard of transparency by requiring clarity and detailed information that must be provided to individuals. Privacy notices will have to be more detailed than they are currently. However, companies selling in several member states will be able to use the same notice template without the need to adapt the notice to local legal requirements. The notice will still need to be translated into the local language, if needed.

Transparency is achieved by keeping the individual informed and this should be done before data is collected and where any subsequent changes are made.

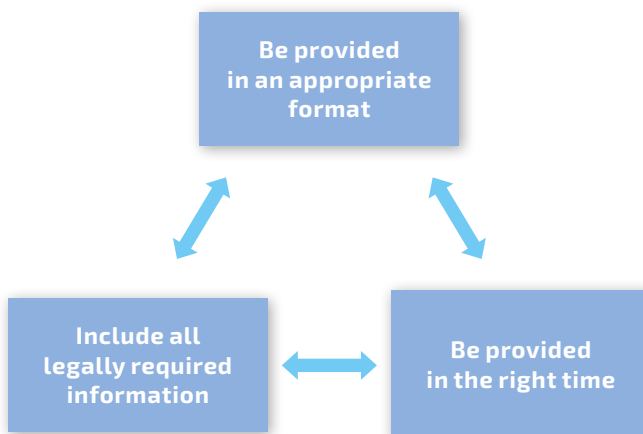
In order to ensure compliance with the new requirements in the GDPR, companies should review all the privacy notice templates provided so far to customers, employees, and any other relevant categories of individuals. Companies may need to create new forms.

#### Is a privacy notice the same thing as a privacy policy?

Privacy information notice (also called privacy statement) is a general term used to describe information provided to individuals about the processing of their personal data. Privacy policy is a form of a privacy notice/statement. The term privacy policy is generally used for longer documents available on the website that describe company's approach to privacy.

#### Key requirements for privacy notice

To be valid under the GDPR, a privacy notice must comply with three general criteria.



The Article 29 Working Party has provided detailed recommendations about these requirements in guidelines on transparency. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

**Guidelines on transparency under Regulation 2016/679, WP 260, rev.01, last revised on 5 April 2017**

#### Format of a privacy notice: key requirements

Under the GDPR key requirements for transparency require that the privacy notice is (Article 12.1):

**Concise, transparent and easily accessible**

**Clear and easy to understand**

**In writing or via other means**

**Free of charge**



## Concise, transparent, intelligible and easily accessible

In practice this means the following:

- Information should be clearly differentiated from other non-privacy related information, such as contractual provisions.
- Information should be easily understandable by an average person.
- Information should outline the consequences of the data processing for the individual.
- Information should be immediately apparent so the individual does not have to seek it out.



*Every website should have a privacy policy.*

- *A link to the privacy policy should be clearly visible on each page of the website.*
- *When personal data is collected online there should be a link to the privacy policy/notice on the same page on which the personal data is collected.*

## Written in a clear and plain language, in particular when information is provided to children

- Information should be provided in as simple a manner as possible, avoiding complex sentence and language structures.
- Information should be concrete and definitive.
- Information should not be phrased in abstract or ambivalent terms or leave room for different interpretations.
- Words such as “may”, “might”, “some”, “often” and “possible” should be avoided.
- Paragraphs and sentences should be well structured, using bullets and indents to signal hierarchical relationships.
- Writing should be in the active instead of the passive voice.
- Information should not contain overly legalistic, technical or specialist language or terminology.
- When information is provided to children, it should ensure that the vocabulary, tone and style of the language is appropriate and resonates with children.



*The following phrases are regarded as not clear:*

*“We may use your personal data to develop new services” (it is unclear what the services are or how the data will help develop them);*

*“We may use your personal data for research purposes”;*

*“We may use your personal data to offer personalised services” (it is unclear what the personalisation entails).”*

## Provided in writing or by other means, including where appropriate, by electronic means

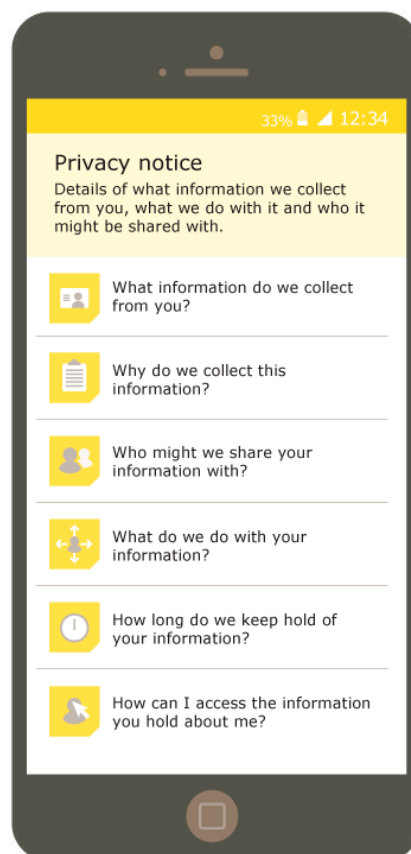
- **In writing:** In printed forms (for example in printed material when providing loyalty card, in printed adverts, on job application forms, etc.)
- **Electronically:** On the website, in text messages, in emails, in apps, including in a layered form. Other electronic means include “just-in-time” contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards.



*The design and layout of the first layer of the privacy notice should provide a clear overview of the information and where/how the individuals can find that detailed information within the layers of the privacy notice.*

*The first layer should always contain information on the processing which has the most impact on the individual, and processing which could surprise him/her. The individual should be able to understand from the first layer what the consequences of the processing will be for him/her.*

A layered privacy notice could look, for example, like this



Source: ICO


- In combination with standardised **icons** in an easily visible, intelligible and legible way, for example via cartoons, infographics, flowcharts, or QR codes printed on internet of things objects.
- Information may also be provided **orally** on request, provided that the individual's identity information is proven by other (i.e. non-oral) means.

## Provided free of charge

Providing information to consumers cannot be made conditional on financial transactions, for example the payment for, or purchase of, services or goods.

## Best practice examples on privacy notice

The UK DPA, the Information Commissioner's Office (ICO), has developed a practical visual on good and bad examples of privacy notices (available [here](#)).



Date of Birth: 10 10 1990  
Occupation: ENGINEER  
Address: 20 STREET, BESDENF/42, CITY TOWN, Post Code: XX 1 0 0 0

**How information about you will be used**  
We may share your information with credit reference agencies and other companies for use in credit decisions, for fraud prevention and to pursue debtors.

We would like to send you information about our own products and services, by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes.

Post ☐ Email ☐ Phone ☐ SMS ☐ Automated phone call ☐

We would also like to share your information with other selected garden products retailers so that they may send you information about their products and services by post. If you agree to your information being shared in this way, please tick the box.


If you need any further information please write to us at 10 Street Name, Town Name, County Name AB123CD.

Customer signature \_\_\_\_\_ Date \_\_\_\_\_

Simple language, clear font and style.

Clear opportunity to agree to marketing.

Prior consent sought for postal marketing by other companies.



Date of Birth: 10 10 1990  
Occupation: ENGINEER  
Address: 20 STREET, BESDENF/42, CITY TOWN, Post Code: XX 1 0 0 0

**LEGAL DECLARATION**  
X Limited is a company incorporated in England and is a member of the X Retail Group ("the Group"). The Group ("we/us") also includes Y Limited and Z Limited and their associated companies from time to time. The personal identifiable information you provide will be processed in accordance with the Data Protection Acts 1984 and 1998 and other applicable laws. We will use your information so that we can process your order. This includes administering any accounts, processing your bank/credit card details in order to obtain payment, arranging delivery of any goods purchased, and the prevention and detection of fraud. We can hand over your information to anyone to whom we transfer our rights and duties under our agreement with you or if we have a duty to do so and the law allows us to do it. We will use your information for market research and the marketing of our products and services. This may include contacting you by post, telephone, email or SMS unless you indicate you do not want to be contacted in any of these ways by calling us on 0870 23 45 67. We will use your information to search the files of credit reference agencies who will record that search. This information may be used by other lenders in making credit decisions about you, members of your household and those with whom you may be financially linked. Information held about you by the credit reference agencies may already be linked to records relating to people with whom you are financially linked. For the purposes of credit searching, you may be treated as financially linked and you will be assessed with reference to any associated records. We will share our information with other companies for the purposes of market research and the marketing of their products and services, unless you indicate that you wish to be excluded from such uses by contacting us on 0870 23 45 67. By signing this form you consent to the information you provide being processed for the above purposes.

Customer Signature \_\_\_\_\_ Date \_\_\_\_\_

Confusing and legalistic language. Closely spaced text, small italic font in light grey.


Unnecessary – means little to the public.

Specific opt-in consent is required for some e-marketing and is good practice for all direct marketing.

Confusing language.

No details of what type of companies.

Bad practice to seek one consent for several types of processing.



**Using your personal information**

6. Personal information which you supply to us may be used in a number of ways, for example:

- To make lending decisions
- For fraud prevention
- For audit and debt collection
- For statistical analysis

(i) We may share your information with, and obtain information about you from, credit reference agencies or fraud prevention agencies, if you apply to us for insurance we will pass your details to the insurer. Information provided by you may be put onto a register of claims and shared with other insurers to prevent fraudulent claims.

(ii) We will not disclose any information to any company outside the XXXX Bank Group except to help prevent fraud, or if required to do so by law


(iii) For further information on how your information is used, how we maintain the security of your information, and your rights to access information we hold on you, please contact: (clear web link/freephone etc.) \_\_\_\_\_

Title that people will understand.

Clarity about who personal information is shared with and why.

Clear info about how to find out more. Easy, free access.

Doesn't describe the companies sufficiently or say how they will provide this marketing information.



**DPA Statement**

6. I/we agree that You and any lender resulting from this application (the "Lender") shall be entitled to use and process, by any medium, the information given by me/us which may be acquired during the lifetime of any loan for the following purposes:

- to provide data and search the files of credit reference agencies or fraud prevention agencies whether before or during the lifetime of any loan granted me/us by the Lender
- to disclose the data to credit reference agencies when required by them for future applications for finance by me/us or my/our financial associates unless I/we successfully file a disassociation with the credit reference agencies.
- to disclose the data to any other company within the XXXX Bank Group or to any third party at any time for the purpose of assessing my/our application and administering and enforcing any subsequent loan
- to disclose the data to any third party who replaces my/our Lender.

By submitting your personal data you CONSENT to it being processed.

We will share information about you within the XXXX Bank Group and also with other selected companies to provide you with information about products/services which we believe may be of interest to you.

Under the terms of the Data Protection Act 1998 you have the right to make a subject access request. All requests must be made in writing to our head office. There is a charge for this service.

If you do not wish to receive marketing information from XXXX Bank Group or other companies please inform your branch.

Title doesn't mean much to the public.

Unnecessarily complicated language. Use of I or me, we or us etc adds to confusion.


Unclear, offputting notice – seems like a difficult, expensive process. People may not know what a subject access request is.

Small print, not easy to do (i.e. contact branch). Opt-out statement not next to statement about marketing information.


## Content of a privacy notice: key requirements

The GDPR lists the following categories of information that must be provided to an individual.


- **Company name and contact details** (email, phone number);
- The identity and contact details of a **DPO** (if appointed);
- The **purposes** and the **legal basis** of the processing;
- If the data processing is based on the **legitimate interest**, an explanation of these interest;

 *As best practice, the company should also provide information from a balancing test, which should have been carried out by the company to demonstrate that there is a legitimate interest and no overriding individual rights.*

- **Categories of personal data** concerned


 *This information is required when personal data have not been obtained directly from the individual, but from other sources. This is because the individual may not be aware exactly which categories of their personal data the company has obtained.*

- **Individuals' rights** (access, rectification, erasure, restriction of processing, objection to processing, portability);


 *This information should include a summary of what the right involves and how the individual can take steps to exercise it. In particular, the right to object must be explicitly brought to the individual's attention and presented clearly and separately from any other information.*

- Whether individuals are being **profiled**;


### Recipients of personal data;

 *The term "recipient" includes other data controllers, joint controllers and processors to whom data is transferred or disclosed. It is recommended that the notice includes information on the actual (named) recipients of the personal data. Where a company only provides the categories of recipients, it must be able to demonstrate why it is fair not to provide names. In such case, the information on the categories of recipients should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.*

- Information on whether personal data is **transferred outside the EEA**;

 *This should specify the relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision, binding corporate rules, standard contractual clauses, and derogations and safeguards). Where possible, there should be a link to the mechanism used, or to the relevant documents. All third countries to which the data will be transferred should be listed.*


- The storage/ **retention period**;

 *The storage period (or criteria to determine it) may depend on statutory requirements or industry guidelines. This must be explained in a way that allows the individual to assess what the retention period will be for specific data and specific purposes. It is not sufficient to state that personal data will be kept as long as necessary for legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.*


- Where processing is based on consent, the **right to withdraw consent** at any time;

 *This information should include how consent may be withdrawn.*

- The right to **lodge a complaint to the DPA**;
- Whether there is a **statutory or contractual requirement to provide personal data**;

 *For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer. Online forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the required fields.*

- The **source of personal data**.

 *Information should include: the nature of the sources (i.e. publicly/ privately held sources; the types of organisation/ industry/sector; and where the information was held (EU or non-EU) etc.). The specific source of the data should be provided unless it is not possible to do so.*

## When a privacy notice needs to be provided

Depending on how the personal data is collected, data controllers have different obligations regarding when to provide a privacy notice.

Although this is not a legal requirement under the GDPR, the Article 29 Working Party recommends providing occasional reminders of the privacy notice.

A data controller may obtain personal data either:

1. **Directly from an individual**, for example by asking the individual to fill in a form (completing an online order, registration for a loyalty programme, hiring an employee).



This includes personal data that:

- An individual provides, for example when completing an online form); or
- A company collects personal data from an individual by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, WIFI tracking, RFID or other types of sensors).

2. **From another source**, for example from another company or buying a database.



This includes personal data obtained from sources such as:

- a. Other companies (third party data controllers);
- b. Publicly available sources;
- c. Data brokers;
- d. Other individuals.

### 4.1.2. Right to access

**Article 15.** An individual has the right to know if the company processes his or her personal data. This means the right to obtain:

- **Confirmation** that the individual's personal data is being processed;
- **Access** to their personal data; and
- **Other information**, including largely what needs to be provided in the privacy notice (See more details in Article 15.1).

The company should verify the identity of the person making the request, using "reasonable means". It means the data requested to confirm the identity should not be excessive.

If the request is made electronically, the company should provide the information in a commonly used electronic format.

A copy of the information must normally be provided free of charge. However, the company may charge a 'reasonable fee' when the access request is:

- Manifestly unfounded or excessive, particularly if it is repetitive; or
- For further copies of the same information that has already been provided.

The fee must be based on the real administrative cost of providing the information.



*In order to be able to respond to access requests, companies are advised to:*

- Put in place rules for keeping data.
- Locate all of the places (databases, filing systems, servers, etc.) where personal data is being stored, so that the company knows exactly where to find the relevant information.
- Maintain records of data flows and use of service providers, including the use of services such as Survey Monkey, or MailChimp, or sharing personal data with the software developers.

### 4.1.3. Right to rectification

**Article 16.** An individual has the right to have personal data rectified if it is inaccurate or incomplete.

A company should respond to such a request without delay, and at least within one month of the receipt. This period can be extended further two months, if the request is complex or there are many requests. The company must inform the individual about such a delay. If a company has shared the data with a data processor (third party) the company must inform them of the rectification where possible.



*In order to be able to comply with rectification requests, companies are advised to:*



- Know where the personal data is stored (paper records, CRM, line of business software, website database, accounts, etc.) so that these systems can be updated.
- Know data flows and data recipients with whom personal data are shared outside the company so they can be informed about the rectification request and they can make relevant corrections.
- Ensure regular data quality checks and review records management systems to identify data correction needs.
- Maintain and regularly update records management policies, with rules for creating and keeping records (including emails).



In order to be able to comply with erasure requests, companies should undertake steps to:

- Establish and regularly review a written data retention policy or schedule outlining when to delete various categories of data and plan for its secure disposal.
- Designate responsibility for retention and disposal to an appropriate person.
- Consider anonymising individual's records if the systems do not allow for data deletion.
- Inform other organisations with whom you shared the data about the erasure request. This applies when you made the data public.

#### 4.1.4. Right to erasure (right to be forgotten)

**Article 17.** An individual has the right to be forgotten and can request the erasure of personal data when:

- The data are no longer necessary for the purposes for which they were collected;
- An individual withdraws consent and there is no other legal ground for processing;
- An individual objects to the processing and there are no overriding legitimate grounds for the processing;



*This case gives companies some degree of flexibility. Not every erasure request must automatically result in data being erased. If a company is able to demonstrate legitimate interest, and there are no overriding individuals' requests, the company might be able to continue to process the contested personal data. For example, a retailer might argue that keeping certain personal data is necessary for handling complaints or product recalls.*

- An individual objects to the processing for marketing purposes;
- The data has been processed unlawfully;
- The data must be erased to comply with legal obligation, and
- The data concerns a child and has been processed in relation to certain online services.

A company may refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise or defence of legal claims.

#### 4.1.5. Right to restriction of processing

**Article 18.** An individual has the right to ask for the restriction of processing of personal data. This right means that an individual can limit the way that a company is processing their data. It is similar to requesting the erasure of the data.

Individuals have the right to request the restriction of the processing of their personal data where:

- An individual questions the accuracy of the data and the company is verifying the accuracy of data.
- The processing is unlawful and the individual opposes the erasure of the data and requests the restriction of their use.
- The company no longer needs the personal data, but the data is still needed for pursuing legal claims.
- An individual has objected to the processing, and the company considers whether its businesses legitimate grounds override those of the individual.

The GDPR suggests a number of ways to restrict the data processing. For example:

- Temporarily move the data to another processing system;
- Make the data unavailable to users; or
- Temporarily remove published data from a website.

Where the processing of personal data has been restricted, the data may only be processed with the individual's consent, and only for limited purposes, such as for the establishment, exercise or defence of legal claims, the protection of the rights of another person, or for important public interest. Otherwise, when processing is restricted, a company can store the personal data, but not further process it.

Often the restriction of processing is only temporary, specifically when the individual has disputed the accuracy of the personal data or the data controller's legitimate interest.

The data controller may lift the restriction. In such case, it must inform the individual before lifting the restriction.



In order to be able to comply with the restriction requests companies are advised to:

- Establish and regularly review procedures to ensure they are able to determine where they may be required to restrict the processing of personal data.
- Have processes in place that enable to restrict personal data if required.
- Ensure that in case of restriction any further processing cannot take place.
- Inform the third parties with whom they shared the data about the restriction request, unless it is impossible, or involves disproportionate effort to do so.

#### 4.1.6. Right to data portability

**Article 20.** An individual has the right to receive personal data that he or she has provided in a structured and commonly used, and machine-readable format. The purpose is to allow the individuals to easily move, copy or transmit personal data from one IT environment to another (whether to individual's own systems or to other data controllers indicated by an individual).

For example, an individual may request that a retailer transmits to another retailer his or her shopping history with the first retailer.

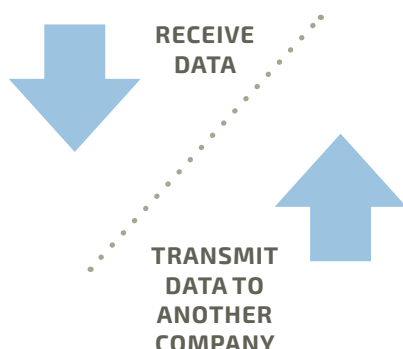
The Article 29 Working Party has issued guidelines on the right to data portability. The following comments reflect these guidelines.

Guidelines from the Article 29 Working Party

**Guidelines on the right to "data portability" WP 242, rev.01, last revised on 5 April 2017**

The right to data portability applies when the data processing is based on consent, or a contract with an individual. The individual does not have the right to data portability if data processing has been based on legitimate interest.

It consists of two forms:



- **Right to receive personal data** and to store those data for personal use, either on a device or in a cloud. For example, an individual might be interested in retrieving his shopping list from a retailer or get information about purchases using different loyalty cards.
- **Right to transmit personal data** from one data controller to another data controller without hindrance, either within the same business sector or to a different one.

The following conditions apply to the exercise of the right to data portability:

- Personal data must **concern the individual making the request**;
- The **individual has provided** the data. In general, this term is interpreted very broadly.
- The right to data portability shall **not adversely affect the rights and freedoms of others**.

According to WP29 guidance, the following data are covered (not covered) by the data portability right

COVERED	NOT COVERED
<p><b>Data actively and knowingly provided</b> by the individual (for example, data requested to set up an account, mailing address, user name, age, etc.).</p> <p><b>Observed data</b> provided by the individual by the use of the service or the device (for example customer's behaviour, such as search history, shopping basket, history of purchases, prices, traffic data and location data).</p>	<p><b>Inferred data and derived data</b>, which are created by the company on the basis of the data provided by the individual.</p> <p>Even if such data may be part of the profile and are inferred, or derived from the analysis of the data provided by the individual, these data will not be considered as data provided by the individual.</p> <p>Data resulting from the analysis of that behaviour and any data created by the company as part of customer profiling, for example for personalisation or recommendation process, is not portable.</p> <p><b>For example, shopping history is portable, but the customer profile created by the retailer is not.</b></p>

## Protection of trade secrets

Exercising the right to data portability must not be used to misuse the information in a way that could be considered an unfair practice, or that would constitute a violation of intellectual property rights. A potential business risk cannot, however, in and of itself, serve as the basis for a refusal to answer the portability request and data controllers can transmit the personal data provided by individuals in a form that does not release information covered by trade secrets or intellectual property rights.

## Managing data portability requests

### Information to individuals


Companies must inform individuals of the right to data portability in the privacy notice.

- Always when personal data are collected directly from an individual (Article 13).
- Always when a company receives the ported data from another company. The receiving company becomes a new data controller but data are not provided directly by an individual (Article 14).

The privacy notice should distinguish the right to data portability from other rights. It is recommended that companies clearly explain the difference between the types of data that an individual can receive through the rights of subject access and data portability.

### How to provide data technically

Personal data should be ported without hindrance from the data controller. Such hindrance could be any legal, technical or financial obstacles that make it impossible or difficult to access, transmit or reuse data by another data controller.

 *For example, according to WP 29, such hindrance could be: fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, or specific and undue or excessive sectorial standardization or accreditation demands.*

If there are technical impediments, the data controller should explain them.

As a minimum, the GDPR requires that personal data be provided "in a structured, commonly used and machine readable format" so that the data can be reused. However, the GDPR does not impose any specific recommendations on the format of the personal data to be provided.

Data controllers are expected to transmit personal data in an interoperable format, although this does not place obligations on other data controllers to support these formats. Where no formats are in common use for a given industry or given context, data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV, ...) along with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction.

The WP29 guidelines include detailed recommendations on the technical aspects of the data portability.



*In order to be able to comply with the portability requests companies are advised to:*

- *Make sure that the data is collected in an organised way, so it can be moved.*
- *Provide an individual with their personal data in a manner that allows them to easily take that data elsewhere.*
- *Provide personal data in a machine-readable format, such as spreadsheet or export file rather than Word document or PDF.*
- *If they do not anticipate many portability requests it should be sufficient to prepare a spreadsheet of a person's data manually and save it as a CSV file.*

## 4.1.7. Right to object

**Article 21.** An individual has the right to object at any time to the processing of his or her personal data if the processing is based on the company's legitimate interest.

Individuals must have an objection on "grounds relating to his or her particular situation".

For processing based on legitimate interest the company must stop processing the personal data unless:

- The company can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

Individuals must be informed about the right to object in a privacy notice in a clear way and separately from any other information.



*In order to be able to comply with the objection requests companies are advised to:*

- *Stop direct marketing immediately upon receiving the objection request.*

- *Ensure that systems are set in a way to remove the objecting individual from the direct marketing distribution list. It may be done by creating a list of objectors either integrated in the centralised CRM or as a separate list to which all relevant systems can refer to.*
- *Make all relevant units in the company aware that an individual who objected should not be subject to further marketing.*
- *Remove an individual who has objected, not only from direct marketing lists but also from the profiling process. For example, if the company analyses data on which customers have not bought from you or visited your store for a certain version, the objecting individual should be removed from such an analysis.*

#### 4.1.8. Right to object to profiling

**Article 22.** Companies that make decisions about individuals based on automated profiling must provide a mechanism whereby the individual can obtain human intervention. That means processes that use profiling must also allow for a manual override.

This is a new right under the GDPR, even if no automatic decision takes place.

When profiling is made for direct marketing purposes, according to WP 29 there is an 'unconditional' right for the individuals to object to profiling. This means that 'there is no need for any balancing of interests'. The company must always honour such requests without questioning the reasons for the objection. In such cases personal data may no longer be processed.

#### 4.1.9. Right to withdraw consent

**Article 7(3).** The controller must ensure that consent can be withdrawn by the individual as easily as giving consent and at any given time. Withdrawal of consent is given a prominent place in the GDPR. The individual must be able to withdraw his/her consent without detriment, this means free of charge or without lowering service levels.

The GDPR does not say that giving and withdrawing consent must always be done through the same action. According to the WP29 guidelines:

- When consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, individuals must, in practice, be able to withdraw that consent equally as easily.
- Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), an individual must be able to withdraw consent via the same electronic interface.

The data controller must inform the individual about:

- The right to withdraw consent before giving consent;
- How to withdraw consent.

#### Impact of withdrawal on data processing

- As a general rule, if consent is withdrawn, all data processing operations that were based on that consent, and took place before the withdrawal, remain lawful. However, the controller must stop any further processing.
- If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted or anonymised.
- If data processing is based on more than one lawful basis, e.g. customer data may be based on contract and consent, withdrawal of consent does not mean a controller must erase data that is processed for a purpose based on the performance of the contract with the individual. Controllers should therefore be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.



*In order to be able to comply with the objection requests companies are advised to:*

- *Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.*
- *Delete data that was processed on the basis of consent once that consent is withdrawn.*
- *Where an individual withdraws consent and the company wishes to continue the processing on another lawful basis, it cannot silently migrate from one consent (which is withdrawn) to another legal basis.*

### Companies' obligations concerning individuals' rights

#### Identification

There are no prescriptive requirements on how to authenticate the individual making the request.

Companies should implement an authentication procedure in order to ascertain the identity of the individual exercising their rights. Where a data controller has reasonable doubts about the identity of an individual, it can request further information to confirm his or her identity.

According to WP29, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate him or her.



For example, user names and passwords are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals chose to use without revealing their full name and identity.

Companies should not request additional information to assess a person's identity and cannot impose demands or collect personal data which is not relevant or necessary.

### **Time limits**

Companies should respond "without undue delay" and in any event "within one month of receipt of the request".

This can be extended to a maximum of three months for complex cases, provided that the individual has been informed about the reasons for such delay within one month of the original request.

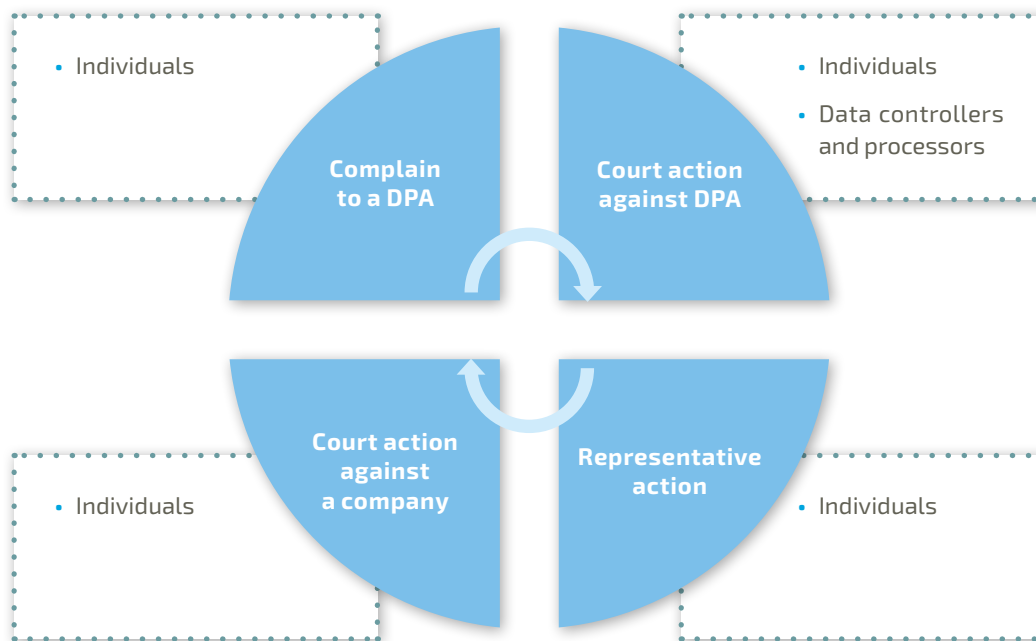
If a company refuses the request, it should inform the individual about the reasons and about the possibility to lodge a complaint with the supervisory authority, not later than a month after receiving the request.

### **Charging a fee for complying with a request**

A data controller should not charge any fees unless it can demonstrate that the individual's requests are manifestly unfounded or excessive, "in particular because of their repetitive character".

## 4.2. Redress and legal claims

### ARTICLE 77-82 OF THE GDPR



**The GDPR takes a multi-layered approach to remedies for breaches of its provisions. Individuals have the right to effective protection of their rights in court and with the DPAs. This includes the right to compensation for damages. The exercise of these rights in court will depend on the national judicial system.**

### **Right to complain to a DPA**

*Available to: Individuals*

Any individual has the right to lodge a complaint with a DPA if he or she considers that his or her personal data has been processed in violation of the Regulation.

The complaint can be filed in the country where the individual lives, works or where the violation took place (Article 77).

### **Right to judicial remedy against a DPA decision**

*Available to: Individuals, controllers and processors*

Each individual or a legal person has the right to an effective judicial remedy against any legally binding decision of a supervisory authority concerning them.

In addition, each individual has the right to an effective judicial remedy where the DPA fails to handle a complaint properly. For example, the DPA refuses to act on a complaint, dismisses a complaint, or does not inform the individual of the progress or outcome of the complaint within three months of it being lodged.

The case against decisions of the DPA must be brought in the courts where the DPA is established. (Article 78).

### **Right to judicial remedy against a controller or a processor**

*Available to: Individuals*

Any individual has the right to a judicial remedy against a data controller or a processor where he or she considers that his or her rights have been infringed.

This right is independent of the right to lodge a complaint with a DPA (Article 79).

It is also independent of the right to call for damages. In practice the individuals will be likely to apply for both a judicial remedy and compensation at the same time.

## **Right to compensation**

### *Available to: Individuals, controllers and processors*

Any person who has suffered material or non-material damage resulting from an infringement of the Regulation has the right to receive compensation for the damage suffered (Article 82).

The right to compensation applies to "any person" and not only a "data subject", which means it applies to both individuals, as well as legal persons (including data controllers and data processors).

A data controller or a processor is liable for both material and non-material damage caused as a result of data processing which infringes the GDPR. A data processor is liable where damage is caused by its breach of a specific obligation imposed on it or where it has acted contrary to instructions received from a data controller.

Material damage is generally quantifiable. There is no definition of non-material damage and it remains to be seen whether any guidance will be given by the European Data Protection Board.

The controller or processor is exempt from liability if it proves that it is not responsible for causing the damage. If more than one controller or processor is responsible for the damage, each of them is liable for the entire damage but they have a right of redress against each other (Article 82).

The case shall be brought before the court of the country where the controller or the processor is established or where the individual lives (Article 82.6 and 79.2).

## **Right to representative action**

### *Available to: Individuals*

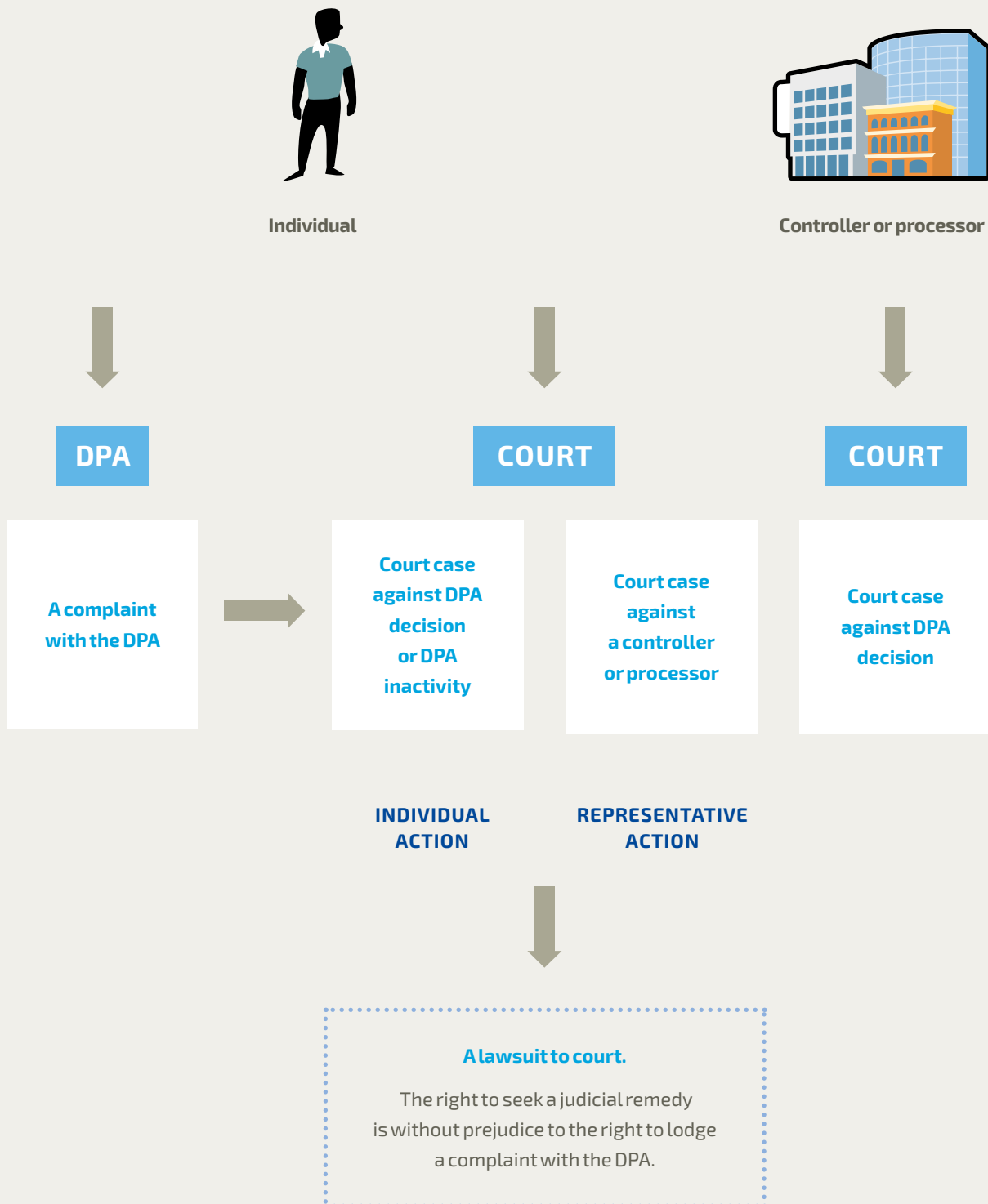
Individuals can request a non-profit body, organisation, or association whose statutory aims are public interest activities in the data protection field to (Article 80.1):

- Lodge a complaint on their behalf;
- Seek judicial remedy against a DPA;
- Seek judicial remedy against a controller or a processor before the court;
- Seek compensation for damage where provided for by Member States law.

The concrete procedure depends on the collective redress system in the Member State concerned. The GDPR does not harmonise procedures in this respect.

Member States may also allow such organisations to lodge collective complaints and relevant actions independently of an individual's mandate (Article 80.2). This means that these organisations do not need any specific request from an individual.

## OVERVIEW OF THE REDRESS SYSTEM UNDER THE GDPR





## THIS CHAPTER COVERED

### Rights

Under the GDPR individuals have the right to:

- Receive information concerning the processing of his or her personal data (Transparency)
- Access the personal data that a company holds about them (Access).
- Obtain the rectification of inaccurate personal data concerning him or her. This also includes the right to have incomplete personal data completed (Rectification).
- Obtain erasure of personal data concerning him or her, where legally permitted (Erasure).
- Obtain restriction of processing of his or her personal data (Restriction).
- Object, on grounds relating to his or her particular situation, to the processing of his or her personal data, including to direct marketing (Objection).
- Receive the personal data concerning him or her, and have the data transmitted to another controller (Portability)
- Not to be subject to automatic decisions producing legal or similarly significant effects, including profiling (Profiling)
- Right to withdraw consent

Companies have to respond to these requests in a timely matter and generally free of charge.

### Redress and legal claims

If individuals think their rights have been violated, they have the right to a judicial remedy before a court and to an administrative remedy before the data protection authority. This includes the right to compensation for damages.



## CHAPTER 5

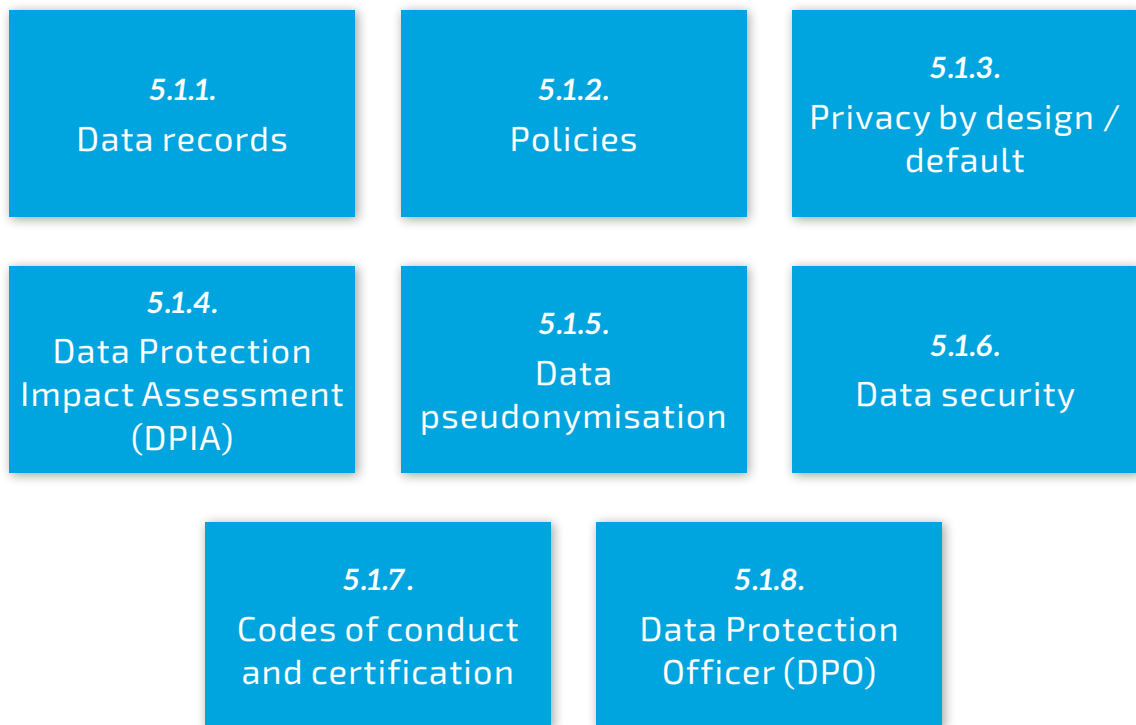
# ACCOUNTABILITY

---

In this chapter: Key accountability requirements • Data Protection Officer

### 5.1. Key accountability requirements

ARTICLE 24, 25 AND 30 OF THE GDPR



***All companies have to implement compliance programmes to ensure that they process personal data in accordance with the GDPR. They also have to demonstrate compliance to the DPAs and the individuals.***

Accountability means implementing various policies and procedures in order to ensure compliance with the GDPR. Accountability entails establishing a culture of proactive monitoring, reviewing and assessing data processing procedures.

The rise in cybercrime, increased data flows, centralisation of databases, as well as technology developments pose increased threats to data privacy and security. Accountability is therefore important for companies in demonstrating that they safeguard privacy as part of maintaining customer trust.

The accountability principle is a core pillar of the GDPR. The Regulation is not prescriptive on what accountability concretely entails. The GDPR generally requires companies to (Article 24):

- Implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and
- Review and update those measures where necessary via internal or external privacy audits.

Measures depend on the risks involved and the nature, scope, context and purposes of the processing. These measures can be different for small and big retailers. A comprehensive accountability privacy program will usually include:

> **Implementing compliance programmes**

- **Specific measures**, including data inventories, internal policies and procedures, privacy policies and notices, data breach handling procedures, security and retention policies, data protection by design or by default, data protection impact assessments, etc.;
- **Audit process** to monitor and revise the effectiveness of the privacy measures in place.
- **Employee training** so that employees with access to personal data understand their roles. This is not a strict GDPR requirement but is recommended.
- An internal **privacy governance structure** for larger organisations.

> **Demonstrating compliance to the DPAs and the individuals.**

### 5.1.1. Data records

An important aspect of demonstrating compliance includes creating and keeping updated records of processing (Article 30). The records have to be made available to DPAs on demand.

The GDPR sets out a detailed list of information that must be recorded, including:

- The name and contact details of the company, and a DPO;
- The purposes of the processing;
- A description of the categories of individuals and of the categories of personal data;
- The categories of recipients with whom personal data are shared;
- The description of transfers of personal data outside the EEA and which safeguards are being used;
- The envisaged time limits for erasure of the different categories of data;
- A general description of the company's security measures.



*Companies employing less than 250 people are exempt from this obligation, unless the processing they carry out is likely to result in a risk to the rights and freedoms of individuals, the processing is not occasional, or the processing includes sensitive data or criminal records. The exemption appears to cover most SME retailers. However, in practice it is recommended that all organisations keep records of processing.*

### 5.1.2. Policies

Companies need to put in place appropriate data protection policies. (Article 24.2). However, the Regulation does not provide any specific details of these policies.

In practice the data protection policies should include a description of:

- Data security
- Data retention periods
- Exercise of individual rights
- Internal access to data.

### 5.1.3. Privacy by design and by default

The GDPR introduces two new concepts of privacy by design and by default, which require companies to consider data privacy throughout the entire lifecycle of all projects and systems that use personal data (Article 25). These concepts help ensure that personal data is only processed if this is necessary and proportionate. However, the Regulation does not provide any details of how these concepts should be implemented in practice.

For retailers, integrating privacy by design and by default will be particularly important in the context of customer loyalty programmes, customer profiling and marketing, and big data analytics.

#### Privacy by design

Privacy by design means that whenever new systems, applications or technologies are developed, the impact on privacy should be considered from the very beginning.

In implementing privacy by design companies can adopt various approaches, including, for example:

- **Data minimisation** – no personal data should be collected unless there is a specific and compelling purpose. This will limit privacy risks at the earliest stage.
- **Data pseudonymisation** – individuals should be made less identifiable, which means that datasets should be stripped of information that could identify an individual either directly or through links to other datasets.
- **User access controls** – access to data should be restricted and this should be combined with other security policies.

Implementing privacy by design should take into account:

- The state of the art;
- The cost of implementation;
- The nature, scope, context and purposes of processing; and
- The risks to rights and freedoms of individuals.





*There are seven broadly recognised privacy by design principles which have not been included in the GDPR. Following these principles might help companies implement practical steps to achieve privacy by design.*

- *Use proactive rather than reactive measures; anticipate and prevent privacy-invasive events before they happen.*
- *Personal data must be automatically protected in any IT system or business practice.*
- *Privacy must be embedded into the design and architecture of IT systems and business practices.*
- *All legitimate interests and objectives are accommodated in a positive-sum manner.*
- *Security is applied throughout the entire lifecycle of the data involved.*
- *All stakeholders are assured that, whatever the business practice or technology involved, it is operated according to the undertakings given by the company, and is subject to independent verification.*
- *Architects and operators must keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options.*

### **Privacy by default**

Privacy by default means that the default settings of systems, applications or technologies should minimise the amount and the sensitivity of personal data processed automatically.

This obligation applies to:

- The amount of personal data collected;
- The extent of their processing;
- The period of their storage; and
- Data accessibility.

### **5.1.4. Data Protection Impact Assessment (DPIA)**

A Data Protection Impact Assessment (DPIA) is a process designed to describe the data processing, assess if it is necessary and proportional, and help manage the related risks. In other words, a DPIA is a process for building and demonstrating compliance.

The Article 29 Working Party has issued guidelines on the Data Protection Impact Assessment. The following comments reflect these guidelines.

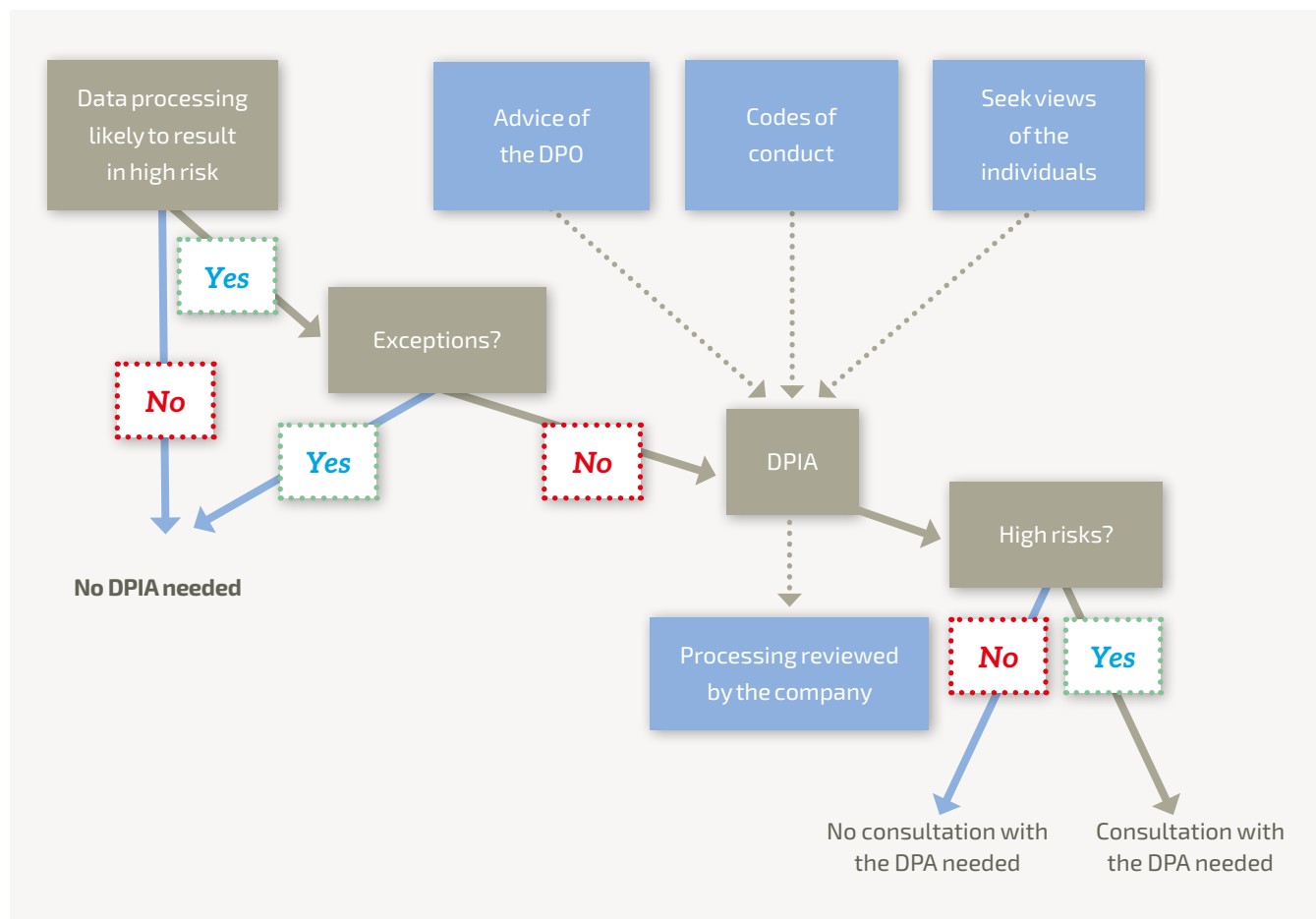
*Guidelines from the Article 29 Working Party*

***Guidelines Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 WP 248, of 4 April 2017, revised on 4 October 2017.***

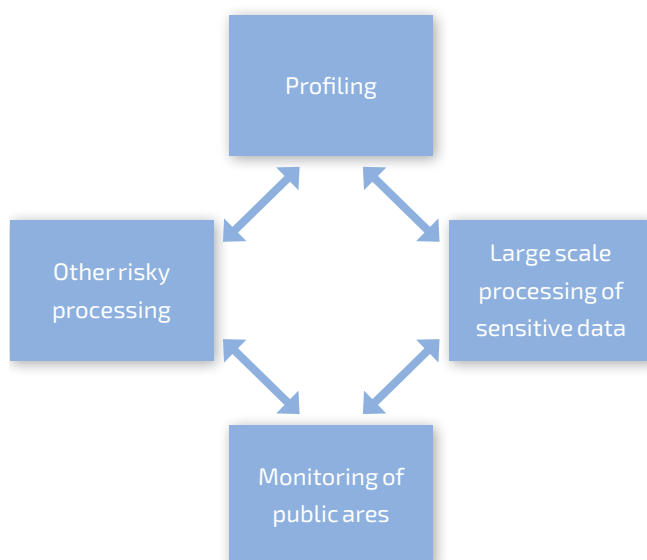
#### **When to carry out a DPIA?**

A DPIA is not mandatory for every processing operation. In line with the risk-based approach enshrined in the GDPR, a DPIA is only required when the processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 35). Where it is not clear whether a DPIA is required, the DPAs recommend performing one nonetheless, as it is a generally a useful tool to help companies comply with data protection law.

## Steps to consider when performing a DPIA



Under the GDPR a DPIA is required in the following cases (the list is not exhaustive and there may be other high risk processing operations which are not mentioned):



- Systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including **profiling**, and on which decisions affecting individuals are based;
- Processing on a **large scale** of sensitive data or criminal records data;

- Systematic **monitoring of a publicly accessible area** on a large scale.

The WP29 guidelines list a number of criteria to consider which processing operations are likely to result in high risk. They include:

- Evaluation or scoring (for example, financial or health risks);
- Automated decision making with legal or similar effects (for example leading to exclusion or discrimination);
- Systematic monitoring (for example, monitoring of publicly accessible area);
- Sensitive data or data of highly personal nature;
- Data processed on a large scale;
- Matching or combining data sets;
- Data concerning vulnerable individuals (for example children, employees, elderly patients, asylum seekers);
- Innovative use or applying new technological or organisational solutions (for example using fingerprint and face recognition);
- When the data processing prevents the individuals from exercising a right.

WP29 recommends that when the data processing meets at least two criteria, a DPIA should be carried out. The more criteria apply the more risky the processing is.

WP29 guidelines provide a number of examples where a particular processing operation may require a DPIA. Two might be relevant for the retail sector:

EXAMPLE	CRITERIA	IS DPIA REQUIRED?
<i>A company systematically monitors its employees' activities, including the monitoring of work station, internet activity, etc.</i>	<i>Systematic monitoring</i>  <i>Data concerning vulnerable individuals</i>	Yes
<i>An e-commerce website displays adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.</i>	<i>Evaluation or scoring</i>	No

A DPIA is not needed for those operations that have been already checked by a DPA under the Data Protection Directive and have not changed since.

A DPIA should be continuously reviewed and regularly re-assessed. Where necessary, in particular when the risks have changed, companies should assess whether the processing complies with the DPIA and whether any DPIA review is necessary (Article 30.11).

#### What should be included in a DPIA?

A DPIA is not formally defined but should include at least:

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of the necessity and proportionality of the processing;
- An assessment of the risks to the rights and freedoms of individuals;
- The measures envisaged to address the risks and demonstrate compliance with the Regulation.

It is sufficient to conduct one DPIA for similar processing operations that present similar high risks.

Companies are flexible in deciding about the structure and form of the DPIA in order to allow for this to fit with existing working practices. However, the methodology should be compliant with the criteria provided in Annex 2 of the WP29 guidelines. Whatever its form, a DPIA must be a genuine assessment of risks, allowing companies to take measures to address them.

#### Consultation

- **DPO.** When carrying out the DPIA companies should consult the DPO. This advice, and the decisions taken by the company should be documented in the DPIA.
- **Individuals.** Where appropriate, companies should also seek the views of individuals concerned or their representatives (for example, trade unions or consumer organisations).

If the final decision differs from the views of the individuals, the company should document its reasons for going ahead. It should also document its justification for not seeking the views of individuals if the company decides that this is not appropriate, for example if it could compromise confidentiality of commercial interests (Article 30.9).

- **DPA.** If the DPIA shows that the personal data processing would result in high risks and no measures have been taken to mitigate the risks, a company should consult the competent DPA before it starts to process personal data.

The DPA has up to eight weeks to provide written advice to the company. This period may be extended by an additional six weeks if the intended processing is complex. The DPA shall inform about the extension within one month after receiving the request.

Formally the DPA does not issue a decision permitting (or not) the processing of personal data, but instead provides advice. However, in practice, companies might need to wait until the DPA issues its advice before starting the data processing.

#### DPIA standards

The DPAs are required to establish and publish a list of the processing operations that require a DPIA. They may also publish a list of those which do not require a DPIA.

### 5.1.5. Data pseudonymisation

The GDPR introduces a new concept of data pseudonymisation. Pseudonymisation means that personal data can no longer be attributed to a specific individual without the use of additional information. The data is neither anonymous nor directly identifiable. The additional information must be kept separately and is subject to strict requirements in order to ensure non-attribution to an identified or identifiable person.

Pseudonymous data is still personal data and therefore, covered by the GDPR. However, companies that render data pseudonymous face lighter compliance regimes in some areas. The GDPR includes incentives to pseudonymise personal data.

- It is easier to process personal data for secondary purposes beyond the original collection purposes (Article 6.4.e).
- It is easier to comply with the data security requirements. In case of a data breach, companies that have pseudonymised personal data may be exempt from the obligation to notify the breach to the affected individuals (Article 34). However, the relevant DPA still needs to be notified.
- Companies do not need to provide individuals with the right of access, rectification, erasure or data portability if they can no longer identify an individual (Article 11). The exemption applies only if the company can demonstrate that it is not in a position to identify the individual and, if possible, it informs the individuals about these practices.

### 5.1.6. Data security

Companies have to ensure the security of personal data and notify data breaches, if they occur (Article 32-34). For more information see chapter 6 below on data security.

### 5.1.7. Codes of conduct

#### Codes of conduct and certification

Adherence to approved codes of conduct and approved certification mechanisms could be used as sufficient demonstration of accountability (Article 40 - 42).

The GDPR acknowledges the use of codes of conduct and the newly introduced certification mechanisms. These tools may help data controllers and data processors to demonstrate compliance with GDPR.



*Data controllers and processors who wish to adhere to the codes of conduct or certification mechanisms are advised to:*

- *Identify or establish associations or representative bodies that could prepare codes of conduct;*
- *Determine whether they intend to adhere to an approved code of conduct or a certification mechanism.*
- *Check the accreditation of monitoring and certification bodies;*
- *Take into account certifications when selecting a data processor(s).*

	CODES OF CONDUCT	CERTIFICATION
<i>Purpose</i>	<p><i>Demonstrating compliance in specific processing contexts.</i></p> <p><i>Enabling data controllers and processors to commit to compliance with recognised standards and practices and be recognised for doing so.</i></p> <p><i>Demonstrating the existence of appropriate safeguards related to the adequacy of data transfers.</i></p>	<p><i>Demonstrating compliance, in particular regarding data security.</i></p> <p><i>Demonstrating the existence of appropriate safeguards related to the adequacy of data transfers.</i></p>
<i>Drafting</i>	<i>Trade associations or representative bodies.</i>	<i>Certification bodies or competent DPA.</i>
<i>Approval</i>	<i>Relevant DPA, and where the processing is cross-border, the European Data Protection Board (the EDPB).</i>	<p><i>Approval takes place on the basis of criteria approved by the relevant DPA or by the EDPB.</i></p> <p><i>Where the criteria are approved by the EDPB, this may result in a common certification, called the European Data Protection Seal.</i></p>
<i>Validity</i>	<i>No restrictions</i>	<i>Maximum three years. Certification may be renewed or withdrawn.</i>
<i>Implications</i>	<p><i>Mandatory monitoring by a body accredited by the DPA.</i></p> <p><i>Adherence may be a mitigating factor when DPA is considering enforcement action.</i></p>	<i>Adherence may be a mitigating factor when DPA is considering enforcement action.</i>

## 5.1.8. Data Protection Officer (DPO)

### ARTICLE 35-37 OF THE GDPR

**Companies that process personal data in certain circumstances must appoint a data protection officer ("DPO"). The DPO is responsible for monitoring compliance with the GDPR and for reporting to the management on privacy-related issues.**

Under the **GDPR**, the DPO is the main pillar of accountability and privacy compliance not only performing a compliance role, but also advising the business and acting as contact point for employees, customers and DPAs.

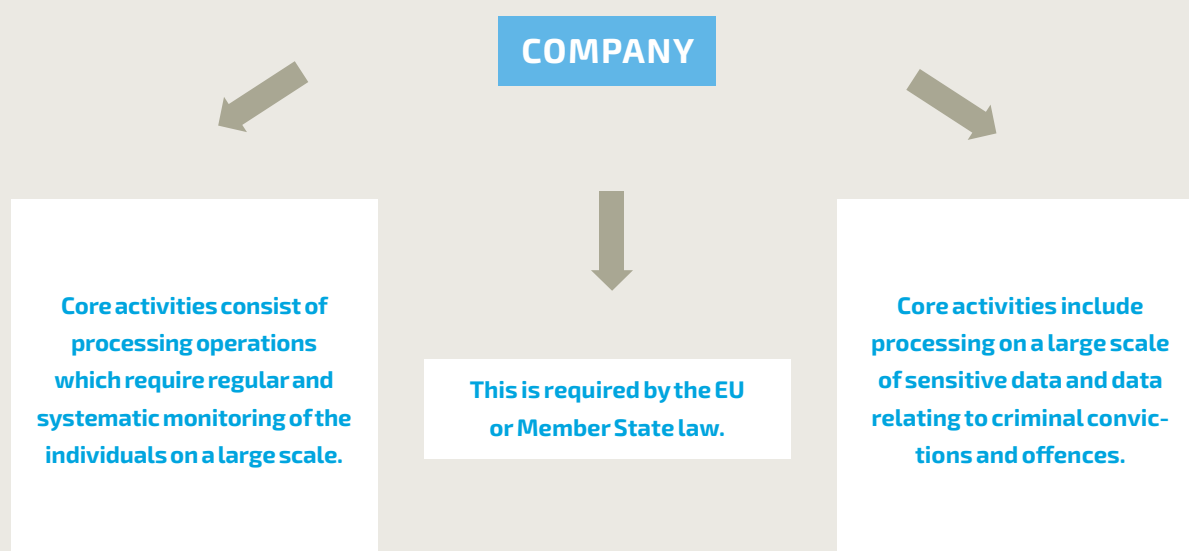
The GDPR requires certain organisations to designate a DPO. This will be the case for all public authorities and bodies, and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

The Article 29 Working Party has issued guidelines on the DPO. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

**Guidelines on Data Protection Officer, WP 243, of 13 December 2016, revised on 5 April 2017.**

### WHEN COMPANIES NEED TO APPOINT A DPO



Companies that are not required to appoint a DPO may appoint one nonetheless.

Companies that do not want to appoint a DPO voluntarily may nevertheless task a member or the team or an external consultant to undertake the DPO tasks. In such a case it should be clear that the title of such person is NOT a data protection officer (DPO).

## DPO appointment

A company will have to appoint a DPO if their core activities consist of processing operations which require regular and systematic monitoring of the individuals on a large scale.



This requirement is vague. The regulatory guidelines from WP29 provide some clarification.

However, most companies will need to make a case-by-case analysis. In cases where it is not clear that a DPO is required, it is recommended that a company documents the reasons for not appointing a DPO.

### Core activities

Core activities are key operations necessary to achieve the company's goals. They relate to primary activities and not to the processing of personal data as ancillary activities.

Some data processing activities are essential and necessary for each company, for example, paying employees' salaries or having standard IT support activities. Such activities would be usually considered ancillary functions rather than core.

### Regular and systematic monitoring

Monitoring is not defined but includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. Monitoring is not limited to the on-line environment. It could also include offline activities.

Some relevant examples of activities that may constitute a regular and systematic monitoring listed by the DPAs include for example:

- **loyalty programs**, email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; behavioural advertising; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.

### Large scale

The following factors may be considered as large scale:

- The number of individuals concerned;
- The volume of data;
- The duration, or permanence, of the data processing activity;
- The geographical extent of the processing activity.

According to the WP 29, examples of large-scale processing include:

- Processing of geolocation data of customers of a fast food chain for statistical purposes;
- Processing of customer data in the regular course of business by an insurance company or a bank;
- Processing of personal data for behavioural advertising by a search engine.

## DPO requirements

### 1. Qualifications and expert knowledge

The GDPR only specifies that the DPO should have:

- Professional qualities, in particular, expert knowledge of data protection law and practices, and
- The ability to fulfil his/her tasks.



- *In practice, this means that the DPO should have expertise in national and EU data protection laws and practices and an in-depth understanding of the GDPR. Knowledge of the business sector and of the company is useful.*
- *The DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the company.*

### 2. Internal or external expert

The DPO may be a staff member or an external consultant.

- If a DPO is an employee, the appointment should be recorded in his/her employment contract, an annex thereto or in a separate document.
- If a DPO is an external person, the appointment should be documented in a service contract.
- The DPO can be either a natural person or a legal entity (for example a consultancy or a law firm).

### 3. Location

A group of companies may appoint a single DPO, provided a DPO is easily accessible from each company's place of establishment.

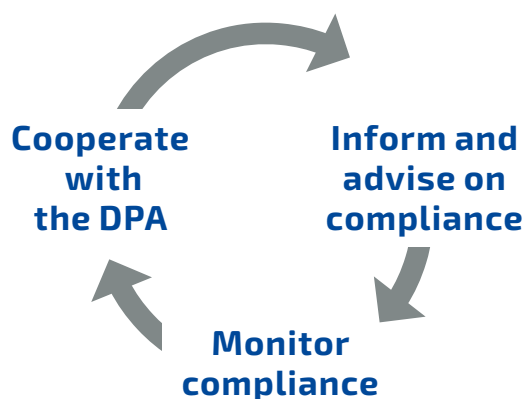
- According to the WP29 guidelines, in order to ensure that the DPO is accessible his/her contact details should be available. The DPO must be able to efficiently communicate with individuals and the DPAs. This also means that the communication must take place in the language used by the DPAs and the individuals concerned.
- The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that individuals will be able to contact the DPO.

### 4. Length of the appointment

This is not specified. The DPO may be appointed for a limited or indefinite term.

#### DPO tasks

When performing his or her tasks the DPO shall have due regard to the risk associated with the processing, and take into account the nature, scope, context and purposes of the processing.



The GDPR requires that the DPO have at least the following tasks (Article 39):

- To inform and advise the company and the employees who are processing personal data of their legal obligations.
- In practice this means providing advice to management and relevant personnel relating to the processing of personal data, such as for example:
  - Liaising with HR in relation to the policies, procedures and practices concerning employees' personal data.
  - Liaising with the IT department in relation to the development of policies, procedures and practices for information security, data handling, outsourcing, and monitoring in the work place.

- Liaising with sales and marketing to ensure compliance with applicable laws and regulations for marketing, and profiling.
- Ensuring that policies concerning access and correction rights are in place.
- Ensuring that written data processing agreements with service providers are in place.

- To monitor compliance with the GDPR and other relevant laws and with the company's data protection policies, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations, and the related audits.

- In practice this may include maintaining an internal register of the processing operations and supervising data processing.
- The DPO should independently verify the company's data protection compliance. This means carrying out audits, making necessary rectifications to internal policies, and reporting deficiencies to the appropriate persons.
- The DPO may also develop procedures to monitor and verify the processing of personal data. This may also include assisting individuals with their access, correction and deletion rights.
- The DPO should ensure that the requests have been handled appropriately and timely. Individuals may contact the DPO on all issues related to the processing of their personal data and the exercise of their rights.

- To provide advice, where requested, on the data protection impact assessment and monitor its performance.

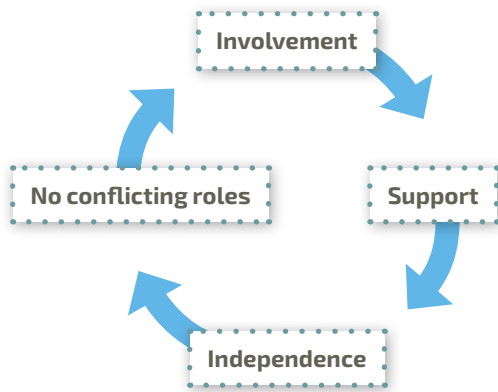
- In practice this may include alerting management of any data protection risks and violations and non-compliance (such as violations of legal requirements, security), and any difficulties the DPO encounters in completing his/her tasks.

- To cooperate with the DPA and to act as a contact point for the DPA for any consultation.

- In practice this means that the DPO should be the contact person for any questions, including on the interpretation and the application of the relevant laws and any other issues.



## The position of a DPO



In order to ensure the DPO's independence, the GDPR provides for safeguards that companies should put in place:

- Ensure that the DPO is properly and in a timely manner involved in all data protection issues.

💡 • This means that a DPO should participate in the meetings of management. DPO presence is recommended where decisions with data protection implications are taken. Relevant information must be passed on to the DPO in order to allow him or her to provide adequate advice.

- The DPO's opinion must be given due weight. In case of disagreement, the reasons for not following the DPO's advice should be documented. The DPO must be promptly consulted once a data breach or another incident has occurred.

- Support the DPO in performing his or her tasks by providing resources necessary to carry out these tasks as well as access to personal data and processing operations, and to maintain his or her expert knowledge.

💡 • The DPO should have sufficient time to fulfil their duties. For example, it is a good practice to determine the time needed to carry out the function and, the appropriate level of priority for DPO duties.

- The DPO should have adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff. The DPO should have necessary access to other services, such as Human Resources, legal, IT, security, etc., so that the DPO can receive essential support, input and information.
- The DPO must have the opportunity to stay up to date with developments within the field of data protection and to increase level of expertise by participating in training courses and other forms of professional development.

- Ensure that the DPO does not receive any instructions from management regarding the exercise of his or her tasks. The DPO shall not be dismissed or sanctioned for performing the tasks. The DPO shall directly report to the highest management level.

💡 • This means that a DPO must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult a DPA. The DPO must not be instructed to take a certain view of an issue related to data protection law.

- Ensure that any additional roles or tasks that the DPO may perform, such as legal, compliance or IT security, do not result in any conflict of interest.

💡 • This means that the DPO cannot hold a position that leads him or her to determine the purposes and the means of the processing of personal data. In general, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the structure.



## THIS CHAPTER COVERED

### **General accountability requirements**

Accountability means implementing various policies and procedures in order to ensure compliance with the GDPR. According to the GDPR, accountability requires establishing internal documentation of the processing of personal data operations, internal data protection policies, Privacy Impact Assessment, privacy by default and by design, ensuring appropriate security, appointing a DPO, and adhering to codes of conduct or certification mechanisms. Accountability implies for the company not only the obligation to comply with the GDPR, but also the obligation to demonstrate to the authorities and/or the individuals how such compliance is ensured.

### **Data Protection Officer**

All companies that process personal data must in certain circumstances appoint a data protection officer ("DPO"). The DPO is responsible for monitoring compliance with the GDPR and reporting to the management on privacy-related issues. Many brick and mortar shops, smaller online shops will not have to appoint a DPO if they do not track or profile their customers on a large scale and this is not "core" to the business. Most companies will need to undertake a case-by-case analysis. In cases where it is not clear that a DPO is required, it is recommended that a company documents the reasons for not appointing a DPO.

## CHAPTER 6

# DATA SECURITY

In this chapter: General data security obligations • Data breaches

### 6.1. Basic information about data security

ARTICLE 32 OF THE GDPR



*Consumers expect that, when making a purchase, the personal data they provide, and in particular financial data, are with a trusted entity with proper security in place. Many retailers process massive amounts of customer data on a daily basis, and many do so from multiple stores across many countries. They are increasingly under pressure to implement security that protects customer data effectively. The fallout from security breaches can be damaging both in direct financial costs as well as in terms of customer trust. The biggest security threats concern leaks of customer databases and their payment details. In recent years, retailers have become one of the most targeted industries when it comes to security threats. Therefore, theft of consumer data has become as important a concern for retailers as merchandise theft.*

One of the core GDPR obligations for all businesses is to ensure data security. Data security is part of the broader accountability requirement.

The security obligation applies both to data controllers and data processors. They are required to implement appropriate technical and organizational measures, taking into account the state of the art, and the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.


In the GDPR, security covers confidentiality, integrity and availability of personal data and should be considered following a risk-based approach: the higher the risk (for the rights and freedoms of individuals), the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk). These risks include accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

## New data security obligations in the GDPR

The GDPR does not define what data security is. In general, data security means protecting personal data (stored in any form: databases, paper files, computers, portable devices, cloud, etc.) from any unwanted actions, such as unauthorised access or modification, accidental loss or destruction. Personal data can be secured in many different ways, including encryption, specific software, backups, or physical security.

### Basic security requirements

There is no one-size-fits-all data security standard. The security measures depend on the particular sector, nature, scope, context and purposes of the data processing or the risks involved in it.

 For example, a brick-and-mortar shop or a small online retailer (with a relatively small number of customers and employees) will have different security risks and different obligations compared to a global omni-channel retailer with operations in many countries.

The GDPR mentions the following basic security measures, without, however, providing any details on how security must be achieved:

- **Pseudonymising** and **encrypting** personal data.
- Ensuring the ongoing **confidentiality, integrity, availability** and resilience of systems and services processing personal data.
- Being able to **restore** the availability and access to data in a timely manner in the event of a physical or technical incident.
- Having a process for **regularly testing**, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Adopting approved codes of conduct or approved certification mechanisms may be used to demonstrate compliance with the security requirements.

### Use of service providers

Engaging service providers has security implications, which the data controller needs to assess, as he will bear liability for any error on the part of the contractor.

Service providers (data processors) must assist data controllers to comply with certain obligations, including general security, breach notification, and data protection impact assessment.

## Industry standards



The best-known standard for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS).

- The ISO 27001 requirements are generic and applicable to all organisations, regardless of type, size or nature.



The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. It has released many guidelines and recommendations on data security including the recent:



**Guidelines for SMEs  
on the security of personal  
data processing**



**Guidelines for SMEs  
on the security of personal  
data processing**

## Basic security checklist

Companies should ensure they have the right physical and technical security in place, backed up by robust policies and procedures, and reliable, well-trained staff. Here are some basic security tips that companies might implement. A key element of any data security policy is to be able to prevent a data breach and, where it occurs, to react to it in a timely manner.

## GDPR Data Security Checklist

1. Make a data inventory
2. Identify the risks and put in place security policies
3. Implement security measures
4. Implement security controls
5. Implement business continuity and incident response procedures

### 6.1.1. Make a data inventory

Map all personal data you process (customer files, contracts, employee data, etc.) and the processing purposes that relate to the data. Map where you hold the data (local servers, cloud, desktop stations, etc.). Look at data flows and the underlying systems that allow the data to be processed, whether internal or external.

### 6.1.2. Identify the risks and put in place security policies

Identify and prioritize risks according to their likelihood and gravity. Examples of risks include theft or loss of a laptop, smartphone or any device carrying personal data, contamination via a malicious code, saturation of communication channels, loss or destruction of paper documents.

Risk-based security ensures that priorities are established and decisions are made through a process of evaluating data sensitivity, system vulnerability and the likelihood of threats.

### 6.1.3. Implement security measures

**Physical Security.** Prevent unauthorized access to systems processing personal data. Data centres, servers, computer rooms, cabinets with data files (employee records) and all media hosting personal data should be secured, cabinets should be locked. Implement systems such as fences, locks, alarm systems, cameras.

**Organizational Security.** Design and organise security to fit the nature of the personal data processed and the harm that may result from a security breach. Be ready to respond to any breach of security swiftly and effectively. Designate a person or a team responsible for ensuring IT security.

**Keep rules up to date** and revise whenever relevant changes are made to the information system that uses or houses personal data, or to how that system is organized. Implement procedures to safely dispose of data.

**Network Security.** Maintain network security, using commercially available equipment and industry standards including firewalls, intrusion detection, prevention systems, access control lists. This may include logical access control (technically implementing the authorization policy, using strong passwords and/or multi-factor authentication); patch management (ensuring the timely rollout of software security updates); secured Internet connections (SSL/TLS technology).

**Encryption.** Ensure, for example via encryption of devices or databases containing personal data (e.g. full disk encryption of laptops and mobile devices), that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage.

**Access Control.** Ensure that only authorized staff can grant, modify or revoke access to an information system that uses or hosts personal data. Define user roles and their privileges, how access is granted, changed and terminated. Apply commercially justifiable physical and electronic security to create and protect passwords.

**Virus and Malware Controls.** Install and maintain anti-virus and malware protection software.

**Personnel.** Implement a security awareness programme and train personnel about their security obligations. This should include training about physical security controls, security practices and security incident reporting. Users must be educated in effective password creation, safe network use and monitored while on corporate networks.

### 6.1.4. Implement security controls

The GDPR provides examples of technical controls that may be appropriate to ensure security appropriate to risk. This may include regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

### ***6.1.5. Implement business continuity and incident response procedures***

Implement appropriate disaster recovery plans. The GDPR requires data controllers to be able to "restore the availability and access to personal data in a timely manner in the event of a physical or technical incident". This involves several steps.

- First, you should ensure that personal data is protected against accidental destruction or loss by making backups.
- You should have a process to detect that a breach has taken place.
- If an incident occurs, you should have a response procedure: who is going to be involved from your team, who decides if, when, and how to inform others of the breach, including customers, DPA, and internal stakeholders?

## 6.2. Personal data breaches

### ARTICLE 33-34 OF THE GDPR

*With the use of digital technology and emerging cyber-crime trends, data breaches occur more often and become more difficult to prevent and track. They may be caused by inadvertent or deliberate actions that result in data being stolen, lost or disclosed, such as theft of storage devices, hacking of computer systems or inadequate data security practices. These data breaches are a real danger for retailers and customers and can affect customer trust. Consumers are becoming more security-savvy and realise that their data is valuable and needs protection. According to various studies, some consumers would stop shopping at a retailer after a breach, or at least take a break from doing so. Therefore, retailers need to take security seriously or they risk losing customers.*

The GDPR introduces a new requirement for a personal data breach to be notified to the competent DPA. In certain cases it is necessary to communicate the breach to the individuals whose personal data have been affected by the breach.

### What is considered a data breach

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Data breaches can occur for different reasons. They may be caused by employees, external parties or IT system errors.

### Types of data breaches

**Confidentiality breach** – an unauthorised or accidental disclosure of, or access to, personal data.

**Integrity breach** – an unauthorised or accidental alteration of personal data.

**Availability breach** – an accidental or unauthorised loss of access to, or destruction of, personal data.

### WHEN A DATA BREACH MAY OCCUR



#### HACKING ATTACK

- Hacking incidents and illegal access to databases containing personal data.
- Theft of computer notebooks, data storage devices or paper records containing personal data out of employees' cars, from hotel lobbies, or of baggage.
- Scams that trick companies into releasing personal data.

#### HUMAN ERROR

- Lost devices and documents: smartphones, laptops, tablets and paper documents.
- Sending personal data to a wrong e-mail or physical address, or disclosing data to a wrong recipient.
- Unauthorised access or disclosure of personal data by employees.
- Improper disposal of any media or documents (hard disk, old account information, customer database, employee pay slips, etc.), into dumpsters (instead of shredders).



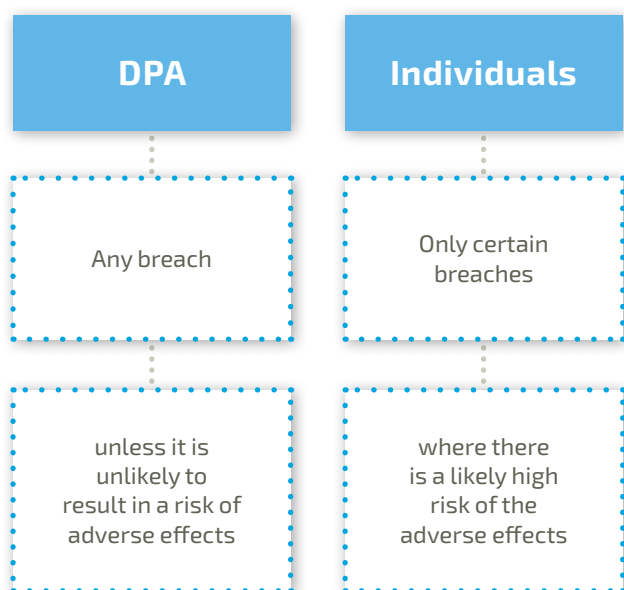
The Article 29 Working Party has issued guidelines on data breach notification. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

***Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 rev. 01, of 3 October 2017, last revised on 6 February 2018.***

## Which data breaches must be notified

Not all data breaches must be notified to the DPA and communicated to the individuals. The GDPR requires the data controller to notify the following breaches:



The threshold for communicating a breach to individuals is higher than for notifying the DPA. Not all breaches need to be communicated to individuals.

Upon becoming aware of a breach, the data controller should:

1. Seek to contain the incident.
2. Assess the risk that could result from the incident.
3. Assess whether notification is required to the DPA and, if necessary, to the individuals concerned.
4. Make the necessary notifications.

## Effects of the breach – the risks

A breach can potentially have a range of adverse effects on individuals, which can result in physical, material, or non-material damage.



Examples of such damage are:

- *loss of control over their personal data or limitation of their rights,*
- *discrimination,*
- *identity theft or fraud,*
- *financial loss,*
- *unauthorized reversal of pseudonymisation,*
- *damage to the reputation,*
- *loss of confidentiality of data protected by professional secrecy, or*
- *any other economic or social disadvantage to the individual concerned. It can also include any other significant economic or social disadvantage to those individuals (Recital 75).*

When assessing the risk, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.

According to the WP29 guidance, a number of criteria should be considered in order to make such an assessment:

- The type of breach (confidentiality, integrity, availability).
- The nature, sensitivity, and volume of personal data. Usually, the more sensitive the data, the higher the risk of harm there is.
- How easy it will be to identify specific individuals, or match the data with other information to identify individuals.
- Severity of consequences for individuals. Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation.
- Special characteristics of the individual, for example, children or other vulnerable individuals.
- Special characteristics of the data controller, for example entities that process sensitive data, such as hospitals, or banks, etc.
- The number of affected individuals. Generally, the higher the number of individuals affected, the greater the impact of a breach can have.



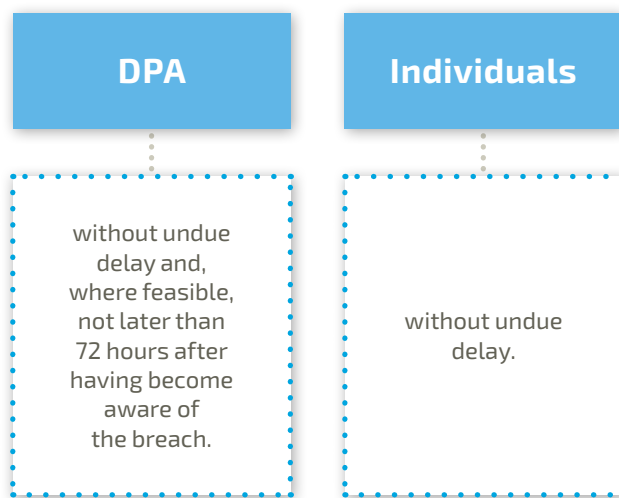
## Outline of data breach notification obligations

### Who must notify

A **data controller**, even if the breach has occurred at a data processor. If a processor engaged by the controller becomes aware of a breach it must notify the controller without undue delay. The data processor does not have its own independent obligation to notify the DPA.

**Joint controllers** shall determine their responsibilities and which party has an obligation to notify in a contract governing their relationship.

### When to notify



The moment of having become aware has not been defined and it depends on the circumstances of the specific breach.

According to the WP29 guidance:

- After discovering a security incident or having received information about a potential breach the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period the controller may not be regarded as being "aware".
- Once the controller has established with a reasonable degree of certainty that a breach has occurred, it has 72 hours to assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered.
- Following this assessment the controller must notify the DPA without undue delay and where feasible not later than 72 hours.

### Which DPA to notify

When a breach takes place across many Member States the data controller will need to notify the Lead DPA.

The Lead DPA is the data protection authority located in the place of the main establishment of the data controller. See Chapter 8 for more information.

Where appropriate, the controller shall indicate whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach.

### Format of the notification

The GDPR does not specify any format for the notification.

According to the WP29 guidance, individuals should be informed by dedicated messages, which should not be sent with other information, such as regular updates, newsletters, or standard messages. Information may be provided via direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media.

A notification solely via a press release or corporate blog is not sufficient. The controller might need to use several methods of communication, rather than using a single contact channel.

### Information to be provided

#### In the notification to the DPA

- The nature of the data breach including where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned. Where precise information is not available, an approximate number of individuals affected may be provided.
- The name and contact details of the DPO or other relevant contact point.
- The likely consequences of the data breach.
- The measures taken or proposed to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

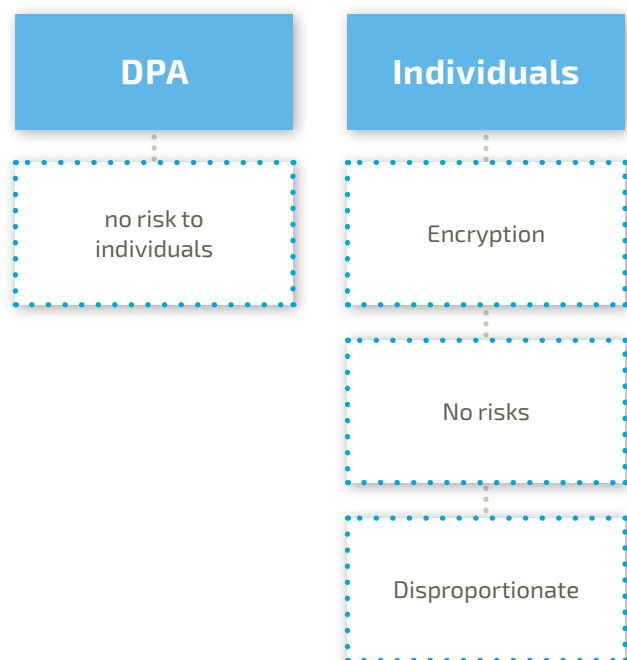
In case of complex breaches where it is not possible to provide all information at once, the notification may be provided in phases. The controller must give reasons for the delay in providing other details at a later stage.

According to the WP29 guidance, in order to avoid being overly burdensome, the controller may submit a bundled notification regarding similar breaches which concern the same type of personal data breached in the same way, over a relatively short time.

## In the communication to individuals

- A description of the nature of the breach.
- The name and contact details of the DPO or other contact point.
- A description of the likely consequences of the breach.
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects, such as resetting passwords.

## Exemptions from notification obligation



### To the DPA

A notification to the DPA is not required if the breach is unlikely to result in a risk to the rights and freedoms of individuals.

According to the WP29 guidance, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the DPA.

An example of a breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device used by the controller and its staff, which means that data was inaccessible to an unauthorised party.

### To the individuals

Communication to individuals is not required if any of the conditions applies:

- **Encryption.** The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.

According to the WP29 guidance communication to individuals is not likely necessary if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible.

- **No risk.** Immediately following a breach, the controller has taken steps to ensure that the high risks posed to the rights of individuals are no longer likely to materialise.
- **Disproportionate.** It would involve disproportionate effort to contact individuals, for example where their contact details have been lost as a result of the breach or are not known in the first place.

Instead, the controller must issue a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.

## Documenting breaches

All breaches must be documented, even if they did not need to be notified.

Breach documentation should include details of the facts around the breach, its causes, and the personal data affected. It should also include the effects and consequences of the breach, and the description of the remedial actions taken. The controller should also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented.

There are no standards regarding the method and structure of the breach documentation. This depends on the data controller. There is also no retention period for how long the documentation should be kept. This depends on the purposes of data processing and the legal bases of personal data that have suffered the breach.

The documentation should be available to the competent DPA.

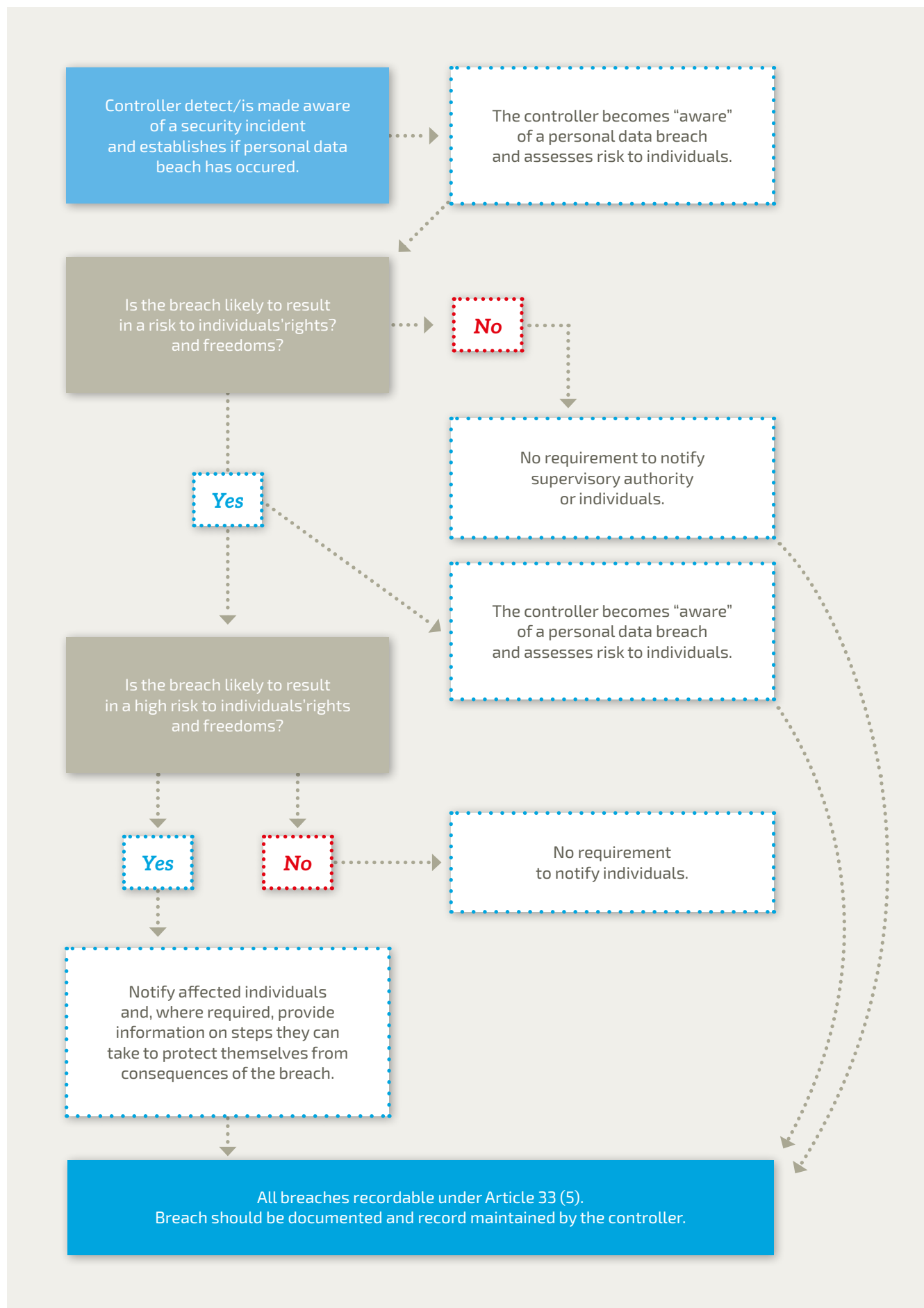
## Examples of notification obligation

(Based on the WP29 guidance)

EXAMPLE	NOTIFICATION OBLIGATION	
	DPA	INDIVIDUALS
A controller maintains an online service. A cyberattack leads to personal data of individuals being exfiltrated.	<b>YES</b>  <i>If there are likely consequences to individuals.</i>	<b>YES</b>  <i>Depending on the nature of the personal data affected and the severity of the consequences.</i>
A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	<b>YES</b>  <i>If a large number of people are affected or if other factors present high risks (e.g. the mail contains the passwords).</i>	<b>YES</b>  <i>Depending on the scope and type of personal data involved and the severity of possible consequences.</i>  <i>Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.</i>
The marketplace operating cross-border suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	<b>YES</b>	<b>YES</b>
A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. As an effect, any user can access the account details of any other user.	<b>YES</b>  <i>The data controller must notify the DPA.</i>  <i>However, the website hosting company, as a data processor, must only notify its affected clients (the data controllers) without undue delay, and not the DPA.</i>	<b>NO</b>  <i>If there is no high risk likely to individuals, they do not need to be informed.</i>

## DATA BREACH NOTIFICATION STEPS

(Based on the WP29 Guidelines on Personal data breach notification under Regulation 2016/679, page. 30, available [here](#).)



## ***Suggested strategies for dealing with data breaches***

Data controllers should put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals, and to determine whether it is necessary to notify the competent DPA, and to communicate the breach to the individuals concerned when necessary. Notification to the DPA should form a part of that incident response plan. Data controllers should consider the following measures.

### **Breach Response Plan**

- Develop and implement a data breach plan, including specific roles and responsibilities with a clear chain of command and employee training to enable a prompt reaction.
- Appoint relevant individuals or create a team to prevent and deal with breaches. It could include IT security, physical security, and legal counsel and HR personnel. Assign clear roles to everyone so that, when a breach occurs, they know how to proceed and who needs to handle various elements of the response plan. Write down instructions, but keep it simple, so that staff actually read it.
- Implement an internal process for detecting and addressing a breach. For example, to find irregularities in data processing, you may use technical measures such as data flow and log analysers, which allow users to define events and alerts by correlating log data.
- Identify upfront the Lead DPA to be notified.
- Consider encrypting the data or implement other measures that will make the data unintelligible. This may limit the obligation to communicate certain breaches to the affected individuals.
- Ensure that agreements with data processors include appropriate security measures. Ensure that these third party service providers are bound by an obligation to inform you immediately about any breach that occurs on their side.

### **Dealing with the breach**

- Gather as much information as possible, including types of compromised data, in particular if the data was sensitive.
- Take initial steps, such as blocking access to and securing personal data as soon as possible. This may involve either physical or IT security measures. Launch an internal investigation, and task the response team with their assigned duties.
- Assess the breach, its scale, the individuals that may be affected and the possible consequences. Prepare a report describing the breach and its scope.
- Where individuals must be notified, establish how many of them are affected, what data types are involved and what risks are involved.
- Determine content and format of information notice in line with legal requirements.

- Notify the competent DPA about the breach within the prescribed timeframe.
- Notify affected individuals about any relevant breach without undue delay. Consider engaging an external service provider where a number of affected individuals to be notified is high.
- Consider engaging a PR agency to analyse media coverage, manage responses, and minimise potential damage to the company's reputation.

### **Document the breach**

- Document any data breach, even those that did not need to be notified.
- You can use your own documentation standards and systems.
- The documentation must be available to the DPA



## THIS CHAPTER COVERED

### General security measures

As cyberattacks are increasing, companies can no longer afford to allow security to be an afterthought. Therefore, it is critical for any company to formulate, implement and maintain, ahead of any breaches, not only appropriate security policies and procedures, but also a breach management strategy. Security needs to be built in from the outset by technical measures such as encryption and tokenisation, access controls and authentication. These need to be supplemented with organisational measures, including appropriate policies, procedures and staff awareness and training.

### Data breach response plan and notification

Companies need to have a broad security plan in place. This should contain action to identify a breach, assess the damage, remove the vulnerability and notify the breach to the DPA and the public. A speedy response can help mitigate damage and the loss of consumer confidence.

All companies will have a general obligation to report any relevant data breaches to a competent DPA without undue delay and where feasible not later than 72 hours after having become aware about the breach. Affected individuals will need to be notified about any relevant breach without undue delay.

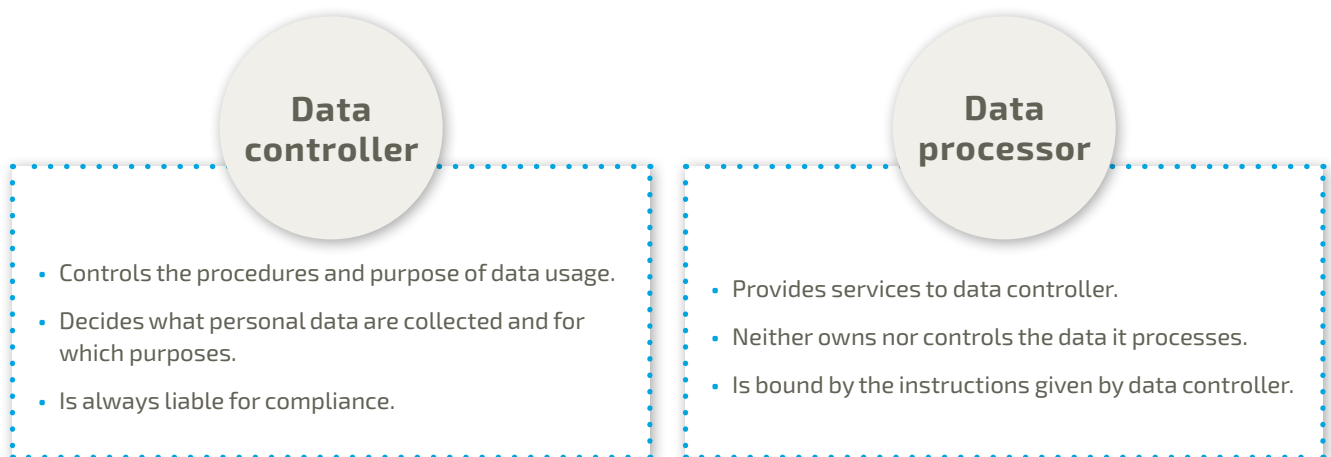
# CHAPTER 7

## DATA FLOWS

In this chapter: Data controller and data processor • Service providers • Data transfers outside the EU

### 7.1. Data controllers and data processors

*The GDPR defines two types of entities that process personal data: data controller and data processor. A data controller and a data processor have different roles and responsibilities. It is important to understand which roles each company engaged in data processing plays. Not all situations are clear-cut, and the same companies may play different roles. For example, if a company simply stores data or provides analytics services for another company, then it the data processor. If the same company receives data from the controller but has flexibility over what kind of analytics services to provide, the analytics company becomes both a data controller and a data processor.*



**Data controller** decides how and why personal data is going to be used by the organisation. The data controller bears full responsibility for complying with the GDPR and for ensuring that individuals' rights are respected and protected.



*In general a data controller decides about issues such as:*

- To collect personal data, which types of data, about whom and how.
- How to use the data and for what purpose.
- Whether to keep the data in-house or to share it with third parties and with whom.
- How long to keep the data and when to dispose of it.

A data controller can process personal data using its own systems but it can also use another company, an external service provider, to provide data processing services. This could be data storage, analytics, etc.

**Data processor** is contracted by a data controller to process personal data on the controller's behalf. In other words, a data processor processes data that the data controller gives them. The data processor can only act in accordance with the instructions given by the data controller and does not have control over the data. This means that the data processor cannot change the purpose and the means in which the data is used.



*For example, a retailer operates an ecommerce website which collects various data on visitors to the website. The retailer is a data controller, because it decides how the collected information is going to be used and for what purpose.*

*The retailer uses Google Analytics to understand the website traffic, how users browse, which pages are most and least popular etc. This information helps the retailer improve content and offers.*

*In such a case Google Analytics is the data processor.*

### Typical responsibilities and functions of data controllers and processors

## Data controller

Comply with the data protection principles, e.g. processing data fairly and lawfully, and using data for specific, legitimate purposes

Provide privacy information to individuals about whom you hold personal data, e.g. your identity, details of the data you hold and what you plan to do with it

Implement security controls and notify about the data breach if it occurs

Conclude written agreements with data processors

## Data processor

Design, create, and implement IT processes and systems that would enable the data controller to gather personal data

Implement security measures that would safeguard personal data

Store personal data gathered by the data controller

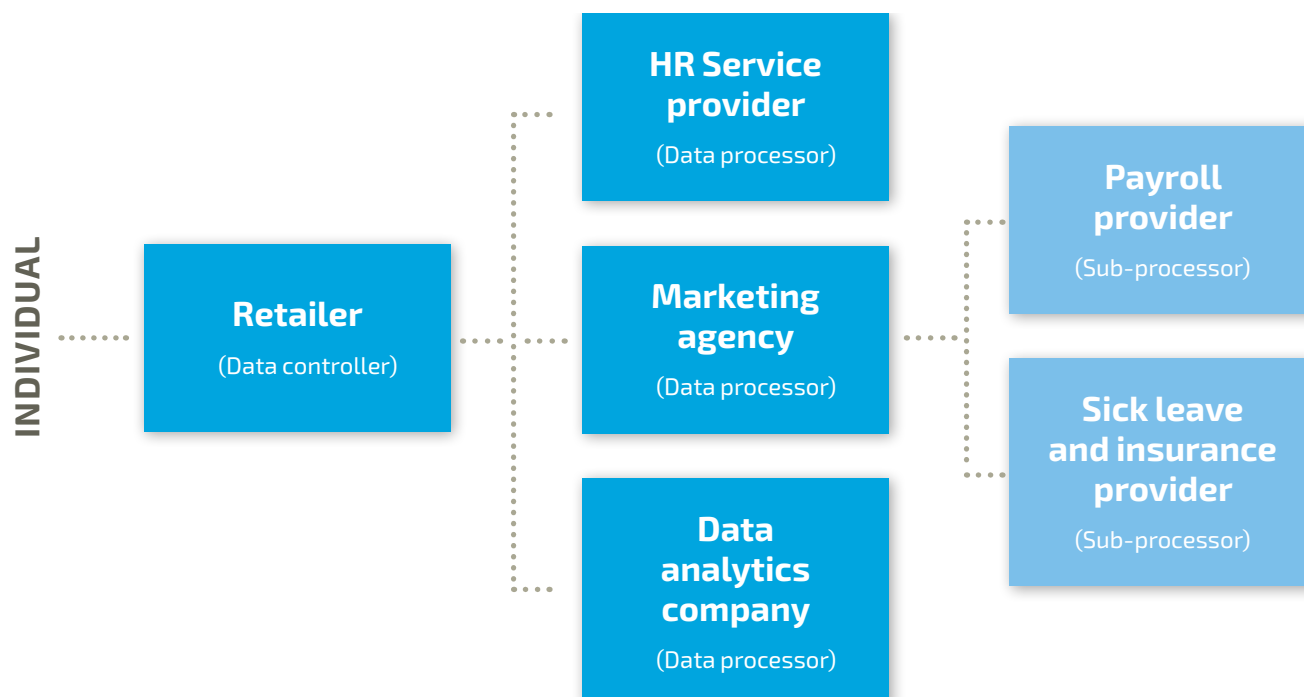
Transfer data from the data controller to another organization and vice versa



## 7.2. Engaging service providers

### ARTICLE 28 OF THE GDPR

#### Example of processing contracts



**Using service providers (data processors) to process personal data requires an appropriate contract committing the service provider to comply with data protection rules. The GDPR imposes detailed obligations and restrictions directly on data processors. There are significant penalties for processors who fail to comply with their new responsibilities.**

The GDPR maintains the rule that a company (data controller) is always responsible for ensuring that personal data processing complies with the Regulation, irrespective of whether it processes personal data in-house or engages a service provider. However, the Regulation will have a significant impact on service providers (data processors) and companies that engage them, as it imposes direct compliance obligations and sanctions on service providers.

Service providers can be either external companies (IT, cloud computing, call centres, accounting, etc.) or other affiliates in the same group.

Retailers typically engage service providers for:

- Processing payroll
- Marketing
- Analytics
- Data warehousing
- IT operations including cloud computing
- Invoicing

- Security and camera surveillance
- Operating call centres

#### New obligations for outsourcing

When selecting a service provider, companies will need to conduct due diligence in choosing a reliable partner. The service provider will need to provide sufficient guarantees regarding data security and act only on the basis of the company's instructions.

#### Contract terms

Companies engaging a service provider (data processor) must ensure this relationship is set out in specific terms in a written contract. The contract must set out the nature and the purpose of the processing, its duration, the type of personal data being processed and categories of individuals concerned, and the obligations and rights of the data processor.

The service providers (data processors) must comply with the following requirements (Article 28.3.):

- Only act on written instructions, in particular where transfer of personal data is prohibited;
- Ensure that the service provider's staff are committed to confidentiality;
- Take all the security measures required by the Regulation;
- Respect subcontracting requirements;

- Assist the company, as far as possible, in the company's own compliance with the exercise of individuals' rights;
- Assist the company in ensuring compliance with the data security, data breach notification, privacy impact assessments, and DPA consultation obligations;
- Delete or return all the personal data after the end of the provision of services and do not process data otherwise; and
- Make available all information necessary to demonstrate compliance with the GDPR concerning outsourcing and allow for and contribute to audits, including inspections.



*The Commission and the DPAs may draft standard contract templates for outsourcing agreements. Companies should stay up to date on any rules and guidance in this area.*

## Subcontracting

If a data processor intends to use a subcontractor, companies must agree to this in writing:

- Either **via a general authorisation**, or the data processor must inform the company of any intended addition or replacement of other processors, so the company may object such changes.
- **Via specific contractual terms.**

The contract between the data processor and the subcontractor must mirror the initial processing contract and include the same data protection obligations as set out in the contract between the company and the initial data processor, in particular regarding data security.

Where a subcontractor fails to fulfil its obligations, the initial data processor is fully liable for any violations.

## Codes of conduct and certification

Companies may only appoint data processors that provide sufficient guarantees they comply with the GDPR. If the data processor has signed up to an approved code of conduct or an approved certification mechanism, this may be sufficient evidence that they are able to fulfil such guarantees.

## Processor's liability – joint controllers

Where a service provider processes personal data other than as instructed by the company, the service provider itself is regarded a data controller and is fully liable as if it were a data controller.



*Companies revising all existing contracts with service providers acting as data processors might take into consideration the following issues:*

- *If you have many agreements to revise identify priority contracts that carry biggest risk.*
- *Determine whether there is a need to renegotiate the contracts or whether a simple addendum with Article 28 requirements will do.*
- *Where do you need tailored amendments consider your negotiation power versus the data processor.*
- *Consider if you should require the data processor to use specific technical measures, such as pseudonymisation or encryption, or implement data protection by design.*
- *In the event of a data breach, require the data processor to notify you about the breach without undue delay, to cooperate with you to investigate and remediate the breach, and cooperate with the relevant DPA, and assist with any notifications.*
- *Consider requiring the data processor to cooperate with:*
  - *any data protection impact assessments (DPIAs),*
  - *any audits or inspections,*
  - *any obligations regarding data security,*
  - *any proceedings with the relevant DPA,*
  - *any individuals' requests concerning their rights,*
  - *any obligations concerning record keeping*
- *Consider whether to modify the indemnities, limits on liability and other similar clauses to address the new risks, including of fines.*

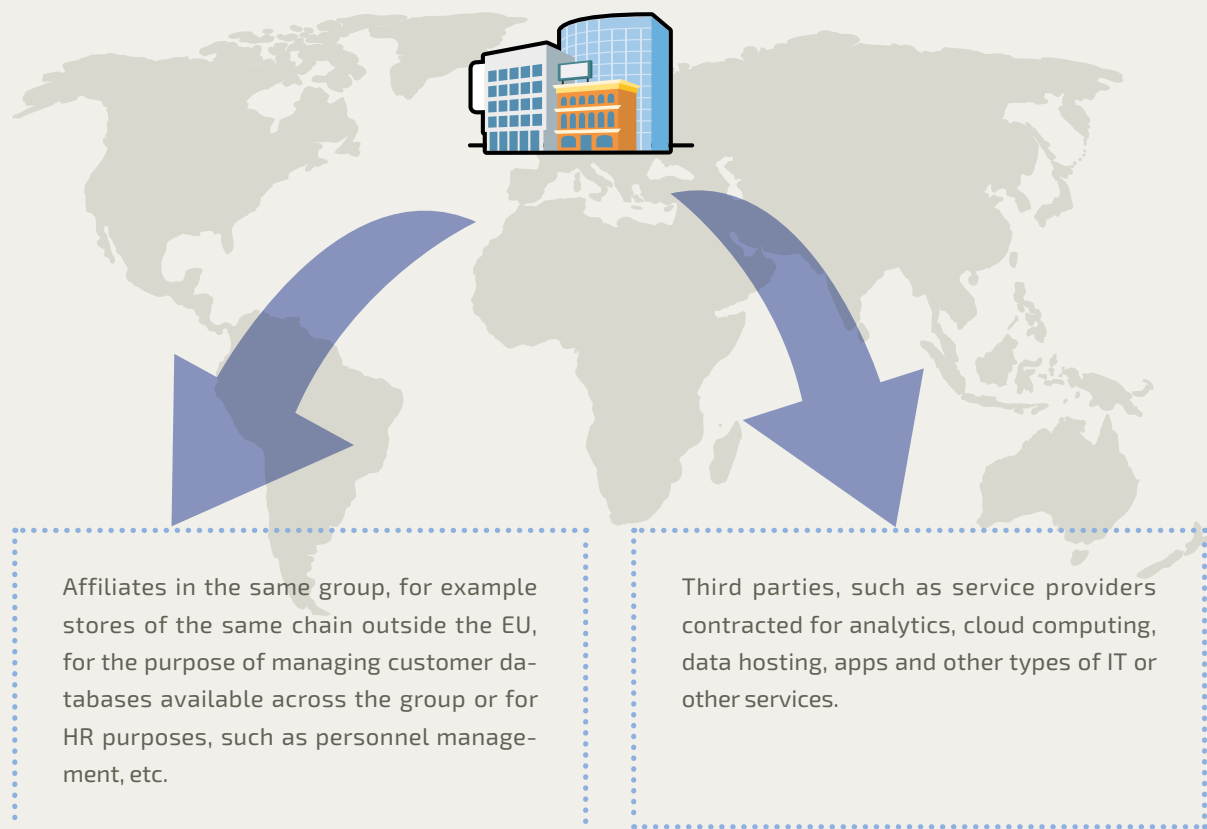
## 7.3. Basic principles on transferring personal data outside the EEA

### ARTICLE 44 - 50 OF THE GDPR

*For any organisation operating in a digital economy the ability to move data across borders, and use data services provided globally is an essential part of business operations. Organisations store customer personal data in a cloud service hosted abroad or may store employee personal data at a subsidiary established in another country. Personal data can flow freely between companies and individuals in the EU. There are, however, restrictions for transferring personal data outside the EU. The GDPR affect such international data transfers.*

**Data transfer** is a form of data processing and concerns any disclosure, distribution, publishing, viewing or access, including remote access to personal data. This means that even if personal data are physically located on a server in the EU, but can be viewed, accessed, copied, etc. by anyone outside of the EU, this is considered to be data transfer.

#### TYPICALLY, DATA TRANSFERS INCLUDE SHARING OF THE PERSONAL DATA WITH AFFILIATES IN THE SAME GROUP AND WITH THIRD PARTIES



The GDPR imposes restrictions on data transfers from companies located in the EU (called in this context **data exporters**) to companies located outside the EU (called in this

context **data recipients**). Such transfers can take place only under strictly defined conditions.

## Overview of the selected data transfer mechanisms

Under the GDPR, the transfer of personal data to recipients outside the EEA is generally prohibited unless:

### 7.3.1. ADEQUACY

### 7.3.2. SAFEGUARDS

### 7.3.3. DEROGATION

Understanding the application of appropriate data transfer mechanisms is essential for all organisations that wish to transfer personal data outside the EEA, including to data processors, such as cloud service providers.

#### 1. Adequacy

**The country in which the data recipient is located ensures an adequate level of data protection (Article 45)**

Under the GDPR, data transfers to countries that are deemed as ensuring an adequate level of protection are regarded as if they were transfers within the EEA. Such transfers can take place without any further protective measures or authorisation from the DPA.

The European Commission, in a special procedure, decides which countries ensure adequate level of protection (adequacy decision). The objective is not to mirror the EU legislation, but rather to establish whether the essential (core) requirements of that legislation are met.

The concept of "adequate level of protection" has existed under the 1995 Data Protection Directive. It has been further developed by the Court of Justice of the EU (Schrems Case (C-362/14)), which said that while the "level of protection" in the third country must be "essentially equivalent" to that in the EU, how it is achieved may differ from the measures existing in the EU. Essential elements of adequacy include: individual rights, obligations for data controllers and data processors, as well as effective enforcement by the data protection authorities.

The following countries outside the EEA have been so far deemed adequate:



#### EUROPE

- Andorra
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- Switzerland



#### NORTH AMERICA

- Canada (only organisations under the Personal Information Protection and Electronic Documents Act (PIPEDA),
- United States (only Privacy Shield certified companies)



#### ASIA

- New Zealand
- Adequacy talks are ongoing with Japan and South Korea.



#### SOUTH AMERICA

- Argentina
- Uruguay

The Commission's decisions adopted under the 1995 Data Protection Directive are valid under the GDPR until they are replaced or repealed. The Commission's decisions shall be reviewed at least every four years. The EU-U.S. Privacy Shield is reviewed annually. The Article 29 Working Party has issued guidelines on adequacy referrals.

*Guidelines from the Article 29 Working Party*

**Working Document on Adequacy Referential (updated), WP 254, adopted on 28 November 2017**

## Privacy Shield

The EU-U.S. Privacy Shield is an adequacy cooperation framework designed by the European Commission and the U.S. Department of Commerce.

It provides companies with a mechanism to comply with EU rules when they transfer personal data from the EU to the U.S. It guarantees that privacy protections for data transferred to the U.S. are equivalent to data protection standards in the EU.

Under the Privacy Shield, companies must self-certify adherence to a set of privacy principles to the U.S. Department of Commerce. These include: (1) the Notice Principle; (2) the Security Principle; (3) the Accountability for Onward Transfer Principle; (4) the Security Principle; (5) the Data Integrity and Purpose Limitation Principle; (6) the Access Principle; and (7) the Recourse, Enforcement, and Liability Principle.

Privacy Shield also includes a detailed set of supplemental principles.

The key elements of Privacy Shield include:

- **Robust enforcement and strong obligations on companies handling Europeans' personal data.** The Department of Commerce will play a more significant role in monitoring certification and ensuring that false claims of Privacy Shield participation are appropriately sanctioned.

Companies that withdraw from Privacy Shield must annually affirm to the Department of Commerce certification to the Privacy Shield principles until the personal data are returned or deleted.

- **Safeguards and transparency obligations on U.S. government access.** Under the Privacy Shield, the U.S. has committed to a new oversight mechanism for national security interference. The oversight is performed by an Ombudsperson that will be independent from the U.S. intelligence authorities. According to the Commission's assessment the Privacy Shield effectively protects EU citizens against generalized access to personal data.

At the time of writing this guide, the U.S. has still to appoint a permanent Ombudsperson, raising questions about the agreement more generally.

- **Effective protection of EU citizens' rights and redress:** The EU individuals may file complaints directly with a U.S. self-certified company, with a free-of-charge independent dispute resolution body, as designated by the company, with national data protection authorities ("DPAs"), or with the Federal Trade Commission ("FTC").

The Privacy Shield includes additional referral options in order to ensure compliance with the privacy principles. Complaints must be resolved by companies within 45 days. If a case is not resolved, an arbitration mechanism, the "Privacy Shield Panel," may be convened to guarantee an enforceable remedy.

- **Annual joint review mechanism.** To monitor and ensure U.S. adherence to commitments on public authority access to personal data, the European Commission and Department of Commerce carry out an annual review, involving DPAs, U.S. national security authorities, and the independent Ombudsperson. The results of this review are published.

The first annual review was concluded in October 2017. Overall, the report has concluded that Privacy Shield continues to ensure an adequate level of protection but some improvements are necessary.

- The U.S. authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield, such as new redress possibilities for EU individuals.
- Complaint-handling and enforcement procedures have been set up, and cooperation with the EU DPAs has been stepped up.
- Relevant safeguards on the U.S. side remain in place regarding access to personal data by U.S. public authorities for national security purposes.

The annual review report is available [here](#)

The second review took place in 2018

Full information from the European Commission on the Privacy Shield Framework is available: [here](#)

Factsheet from the Department of Commerce: [here](#)

## 2. Safeguards

**The data exporter has to put in place adequate safeguards (Article 46, 47).**

The GDPR sets out several options under which transfers can take place to countries that do not provide an adequate level of protection. Such transfers may take place with the following safeguards:

**Binding Corporate Rules (BCRs)**

**Standard Contractual Clauses (SCC) and other contracts**

**Codes of Conduct**

## 2.1. The Binding Corporate Rules (BCRs)

BCRs are internal rules adopted by a multinational group of companies which define the groups' global policy on the transfers of personal data within the same corporate group to entities in countries which do not provide an adequate level of protection. Personal data can then be transferred from organisations within the EU to their affiliates outside of the EU. BCRs must be approved by the DPAs.

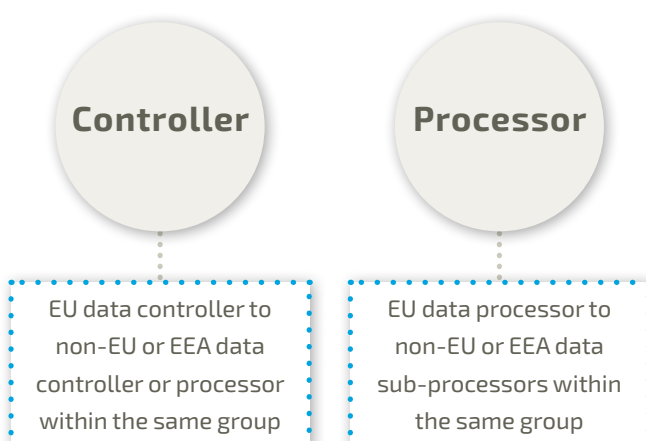
BCRs have existed before under a special procedure developed by the Article 29 Working Party. The GDPR now formalises this procedure by setting out harmonised rules BCRs approval by the competent (Lead) DPA.

BCRs do not cover transfers of personal data outside a corporate group, for example to a service provider. Other mechanisms must be used for such transfers.

Under the GDPR, BCRs must:

- Be legally binding and apply to and enforced by every company in the group;
- Confer enforceable rights on individuals with regard to the processing of their personal data;
- Contain detailed information, such as:
  - > The structure and details of the group;
  - > Description of data transfers including the categories of personal data; the type of processing and its purposes; the type of individuals affected; the third countries where transfers take place;
  - > The application of the general data protection principles;
  - > The individuals' rights and how they can be exercised, particularly the right to lodge a complaint with the competent supervisory authority or before the competent court and the internal complaint procedure;
  - > The acceptance of liability by the EU-based company for any breaches of the BCRs by a group member established outside the EU
  - > Other details (Article 47).

There are two different types of BCRs



The Article 29 Working Party has issued guidelines on BCRs. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

**Working Document setting up a table with the elements and principles to be found in the Binding Corporate Rules, WP 256, adopted on 29 November 2017**

**Working Document setting up a table with the elements and principles to be found in the Processor Binding Corporate Rules, WP 25, adopted on 29 November 2017**

The WP29 working documents include practical tables setting out the elements and principles to be included in the BCRs. These tables clarify information that must be included in BCRs under the GDPR. They also distinguish between information to be included in BCRs and information to be included in the application for the BCR approval by the DPA.

Existing BCRs authorisations remain valid under the GDPR until amended, replaced or repealed by the DPA who made them.

Nevertheless, WP29 recommends bringing the existing BCRs in line with the GDPR. Group companies should notify any relevant changes to their BCRs to all other entities in the group and to the lead DPA as part of their annual update.

## 2.2. Contractual clauses

There are two ways in which contractual arrangement between the parties can be used to provide adequate safeguards:

- **Standard contractual clauses (SCC)** adopted by the Commission or by a DPA (and approved by the Commission) are used.
- **Ad hoc contractual clauses** approved by the DPA are used.

The SCC are a contract template adopted by the Commission or by the DPA. They include a set of template contractual terms concerning rights and obligations of the data exporter and data recipient as well as liability for violations. Each contract needs to contain an annex with a detailed description of the transfer including categories of personal data transferred, data recipients and purposes of the transfer. Companies may not deviate from this standard template.

The standard contractual clauses can be included in a general commercial agreement between the data exporter and data recipient.



There are two different types of SCC:

#### **EU data controller to non-EU or EEA data controller (C2C)**

- [decision 2001/497/EC](#)
- [decision 2004/915/EC](#)

#### **EU data controller to non-EU or EEA data processor (C2P)**

- [decision 2010/87/EU](#)

There are certain advantages to relying on the SCC. For example, they are relatively easy to draft. However, the SCC are static documents that cover only a concrete data transfer with a limited set of personal data and transfer purposes. For complex data flows, keeping track of the changes may become burdensome.

### **2. 3. Approved code of conduct or certification**

The GDPR provides for the use of codes of conduct or an approved certification mechanism, not only as a tool to demonstrate compliance, but also as a transfer mechanism. In order to provide adequate safeguards, the adherence to an approved code of conduct or a certification mechanism must be combined with binding and enforceable commitments by a data recipient (data controller or processor) outside the EEA to apply the appropriate safeguards.

The codes of conduct or certification may be prepared by associations or other bodies representing controllers or processors. They must be approved by the DPAs.

### **3 . Derogations**

#### **There is a specific derogation or exemption (Article 49)**

The GDPR also provides for a number of derogations which can serve as a data transfer mechanism (Article 49). These derogations are similar to the derogations under the 1995 Data Protection Directive. Some of these derogations also largely correspond with the legal bases for data processing included in Article 6 of the GDPR. However, as a data transfer mechanism the derogations are interpreted narrowly and can be relied upon under strict conditions.

They include:

- Consent
- Contractual necessity
- Important public reason
- Establishment and exercise of legal claims
- Protection of individual's vital interest
- Transfer is made from a public register

The European Data Protection Board recommends a layered approach to data transfers. This means that the data exporter should first consider providing adequate safeguards (BCRs, contracts or codes of conduct) and only in their absence use the derogations provided in Article 49.

The Data Protection Board has issued guidelines on derogations. These were the first guidelines adopted under the GDPR. The following comments reflect these guidelines.

*Guidelines from the European Data Protection Board*

***Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018***

If the transfer cannot be based on the standard contractual clauses, BCRs or any of the other derogations set out above, the transfer may exceptionally take place based on the legitimate interest of the company, if the transfer is not repetitive and concerns a limited number of individuals. The DPA must be informed about the transfer, which does not mean that the transfer needs to be authorized by the DPA. This final derogation allows for some flexibility, but also requires a careful assessment and proper documentation and should only be applied as an exception.



## THIS CHAPTER COVERED

### **Engaging service providers**

The Regulation imposes detailed obligations and restrictions directly on processors. There are significant penalties for processors who fail to comply with their new responsibilities. The new law is prescriptive in relation to the detailed contracts that need to be in place whenever a service provider is engaged. The Commission and the DPAs may draft standard contract templates for outsourcing agreements. Companies should stay up to date on any developments.

### **Transfers of personal data outside the EU**

There are restrictions on transferring personal data outside the EEA, unless the third country to which personal data are transferred ensures an adequate level of protection. If companies want to transfer personal data to companies located in countries that have not been deemed adequate, they must put in place adequate safeguards, including contractual agreements, or Binding Corporate Rules, or choose data recipients in the U.S. that have certified with the Privacy Shield.



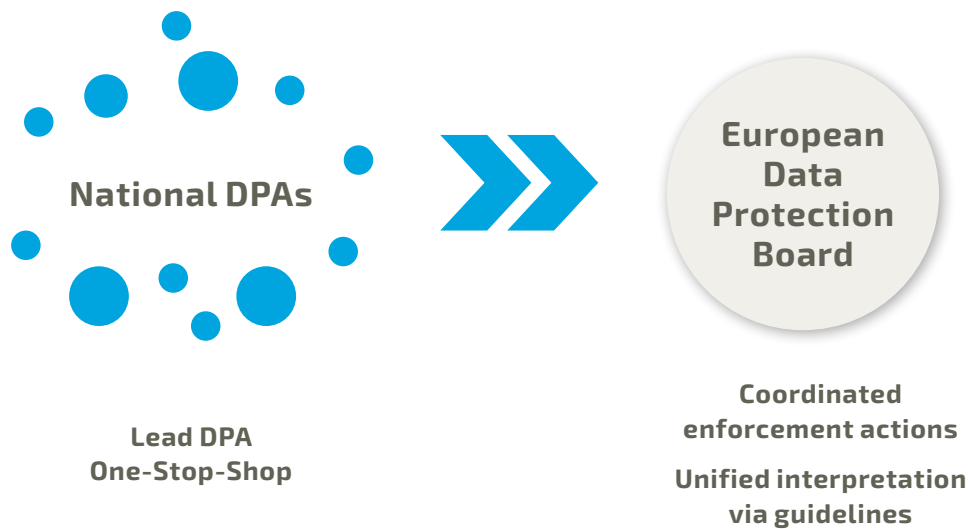
## CHAPTER 8

# ENFORCEMENT

In this chapter: Data Protection Board • Lead Data Protection Authority (DPA) • One-Stop-Shop • Sanctions

### 8.1. Data Protection Authorities (DPAs) and One-Stop-Shop

ARTICLE 51-79 OF THE GDPR



*The GDPR has increased enforcement powers of the Data Protection Authorities (DPAs) including a power to impose significant fines, and a much more coordinated and consistent decision-making mechanism. The size and type of a company or the nature of the company's business makes no difference to the ability of DPAs to enforce the law, so both small and large retailers risk enforcement in case of non-compliance.*

In addition to more stringent enforcement powers, the GDPR also formalises enforcement in order to make it more consistent and more effective.

The GDPR does this by creating:

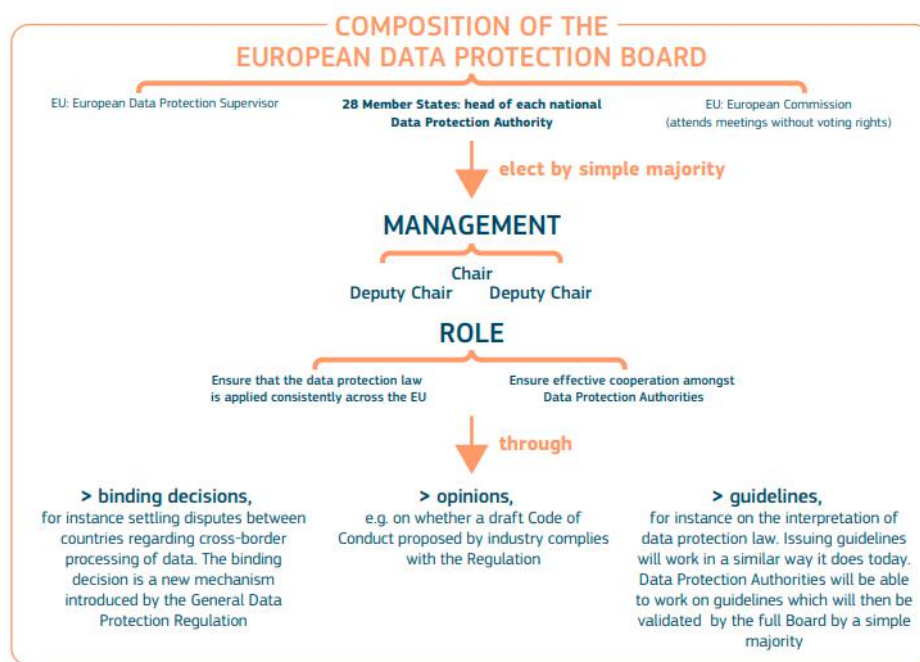
- The **European Data Protection Board (EDPB)**, which replaces the Article 29 Working Party (WP29).
- A new coordinated decision making system via **One-Stop-Shop** procedure and a function of the **Lead DPA**.

## Data Protection Board

The EDPB is composed of the heads of one data protection authority (DPA) of each Member State and of the European Data Protection Supervisor, or their respective representatives.

Under the GDPR, the EDPB has been institutionalised and has now legal personality.

The EDPB's main role is to ensure consistent application of the GDPR, issue binding decisions, issue guidelines and recommendations and best practices (full list of EDPB tasks is included in Article 70).



Source: [European Commission](#)

## Lead Data Protection Authority and One-Stop-Shop

A novelty of the GDPR is that a company operating in several Member States is subject to the authority of one Lead DPA, supervising all cross-border processing activities of this company.

This is known as the One-Stop-Shop mechanism. It aims at simplifying the way companies with operations in multiple EU countries interact with the DPAs.

The Lead DPA will coordinate operations involving the authorities concerned, (e.g. One-Stop-Shop, mutual assistance, and joint operations). It will submit any draft decision to those authorities with an interest in the matter. For more information see section below on coordinated enforcement actions.

The Article 29 Working Party has issued guidelines on the Lead DPA and One-Stop-Shop. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

**Guidelines for identifying a controller or processor's lead supervisory authority, WP 244 rev.01, last revised 5 April 2017**

## When do the One-Stop-Shop rules apply?

The One-Stop-Shop mechanism and the Lead DPA rules apply only where a data controller or a data processor carries out cross-border processing of personal data. This means:

- Data processing takes place in the context of the activities of establishments in **more than one Member State** (for example, a retailer operates a retail chain in a few Member States selling to consumers across these countries).
- Data processing takes place in the context of the activities in **one EU establishment, but it substantially affects or is likely to affect individuals in other EU Member States** (for example, a retailer has an online shop in one Member State but sells across the EU).

To determine whether a processing activity may substantially affect individuals in more than one EU country, companies need to take into account whether the processing (some examples):

- Causes damage, loss or distress to individuals;
- Limits individuals' rights and opportunities;
- Affect individuals' financial or economic status or circumstances;
- Leaves individuals' open to discrimination or unfair treatment;
- Causes individuals' to change their behaviour in a significant way;
- Creates unlikely, unanticipated or unwanted consequences for individuals;
- Creates embarrassment or other negative outcomes including reputational damage, or;
- Involves the processing of a "wide range" of personal data.

The One-Stop-Shop mechanism **does not apply to companies**:

- Only with **local data processing**, for example, a brick-and-mortar shop established only in one country.
- **Not legally established in the EU**, even if they have a representative in the EU. In this case company must deal with each and every DPA in a country where it operates.

## Lead DPA - Main Establishment

The Lead DPA is the data protection authority located in the place of main establishment of the data controller or data processor. This means:

- For companies with single establishment – the Lead DPA of that place of establishment.
- For companies with several establishments in the EU:
  - > The Lead DPA is the **DPA of the central administration (headquarters)**, in the country where the company is located.
  - > The Lead DPA is the **DPA of another country of establishment if this part of the company takes decisions about data processing and has the power to have such decisions implemented**. This means, one company may have multiple Lead DPAs, for example a company's direct marketing decisions are made in one location and analytics in another.

It is up to each company to decide on their main place of establishment. However, such decisions can be challenged. Therefore, companies should be able to demonstrate effective and real exercise of management activity or authority over personal data.

The regulators encourage companies to streamline their data processing decision making powers via single location to avoid or limit a multiplication of Lead DPAs.

The following factors may be helpful in making a decision about the location of central administration:

- Final sign off is given on the purposes and means of the cross-border processing activity;
- The director(s) with management responsibility is/are located there for the cross-border processing activity in question;
- Business decisions involving data processing are taken there;
- The power to implement the decisions lies there;
- A company has registered its processing activities there if in a single territory;

Any other factors apply, which companies consider relevant in the context of the specific activity they carry out.

The rules are similar for data controllers and processors. In cases involving both a controller and a processor, the Lead DPA will be that of the controller.

## Obligations towards Lead DPA

Companies must:

- Register their data protection officer with the Lead DPA;
- Consult the Lead DPA in relation to processing activities which may result in a high risk to individuals,
- Notify the Lead DPA of a data breach where breach reporting is required.

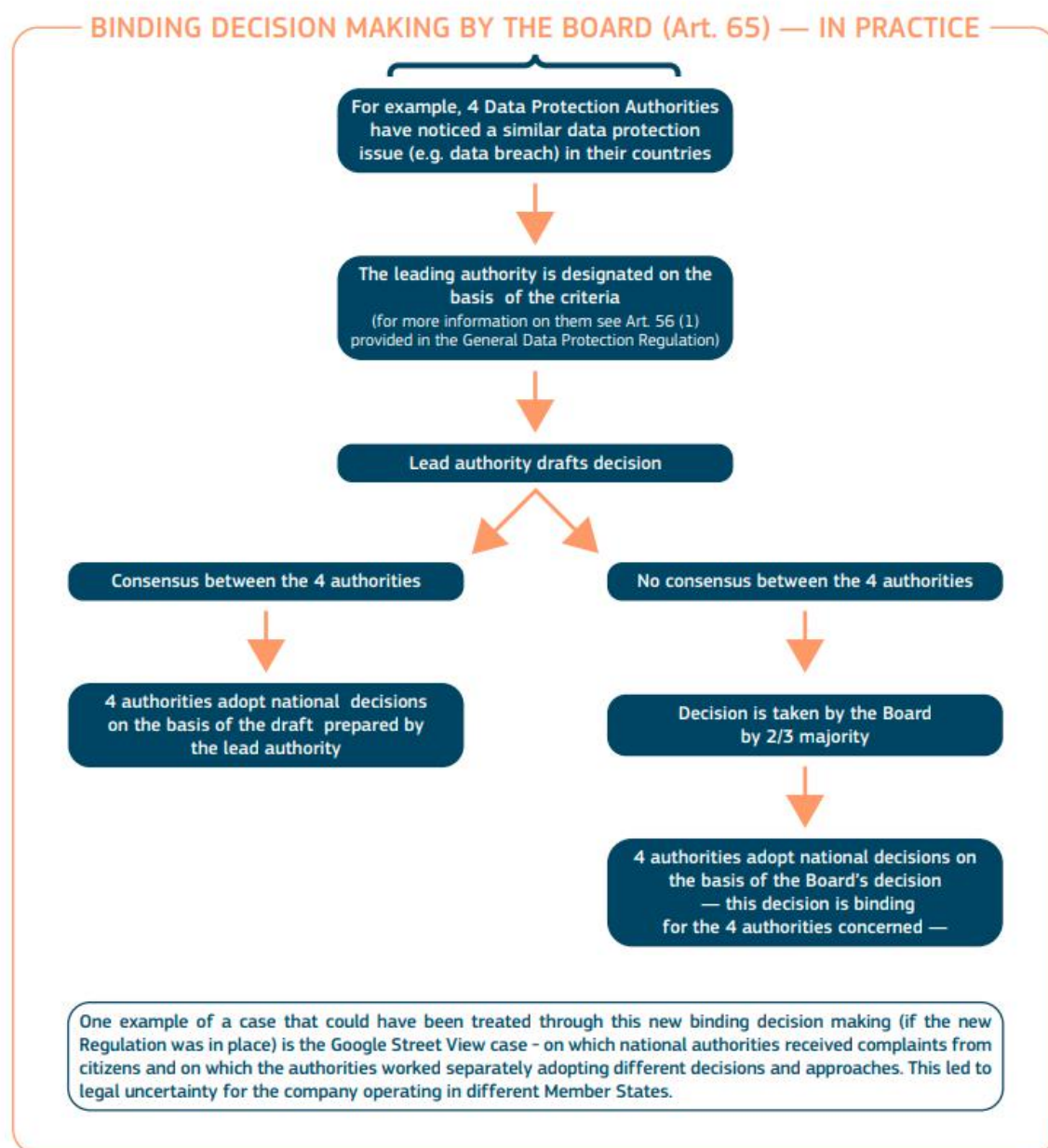
## Coordination of enforcement actions and other activities and binding decisions among the DPAs

A Lead DPA will coordinate operations involving local DPAs in the context of joint operations or investigations.

The Lead DPA will also have primary responsibility for dealing with a complaint from an individual in cross-border cases.

Other concerned DPAs remain competent to investigate and enforce the GDPR if a complaint is directed to them, or if there is an infringement within their Member State or which substantially affects only individuals located within the Member State, unless the Lead DPA decides to take over the case.

If a DPA wants to initiate an investigation despite not being the Lead DPA, it must notify the Lead DPA about its intentions. The Lead DPA then has three weeks to determine whether it wishes to intervene and apply the co-operation procedure. If it wishes to intervene, the DPA can produce a draft decision for the Lead DPA's consideration. If the Lead DPA does not wish to intervene, this first DPA will carry out the investigation on its own.

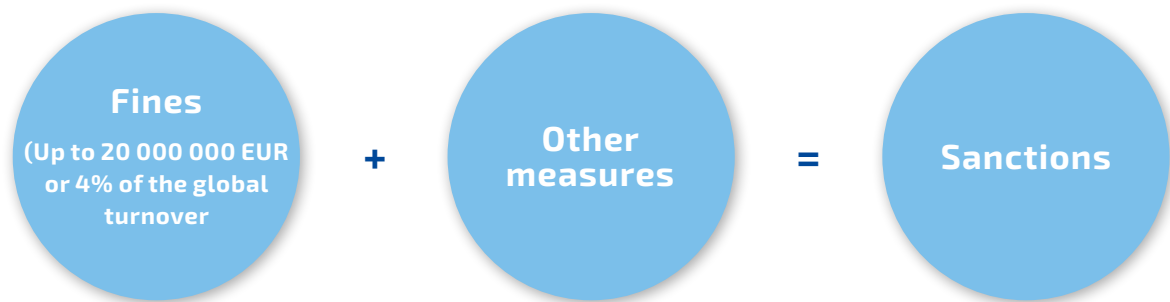


Source:

[European Commission](#)

## 8.2. Sanctions

### ARTICLE 83-84 OF THE GDPR



**Organisations violating the GDPR will face penalties and sanctions which, combined, are significantly more severe than any current national system. Under the GDPR each DPA can impose fines in addition to, or instead of, corrective measures. Maximum fines can reach up to 4% of a company's annual global turnover or 20 million EUR, whichever is greater. In addition, there are other sanctions mechanisms, such as a prohibition on data processing, which can have far reaching consequences.**

### The DPAs enforcement powers

Under the GDPR, the DPAs have a number of investigative and corrective powers. Some of the corrective powers have a potentially significant impact on daily operations, including powers to ban the processing or suspend data transfers to third countries.

Some of these powers can be applied to both controllers and processors.

#### The DPAs have **investigative powers** to:

- Order a data controller/processor to provide any information that the DPA requires for the performance of its tasks;
- Carry out data protection audits;
- Review certifications;
- Notify a data controller/processor of any alleged infringement of the GDPR;
- Obtain from a data controller/processor access to all personal data and all information necessary to perform its tasks; and
- Obtain access to any premises of a data controller/ processor including data processing equipment.

#### The DPAs have **corrective powers** to:

- Issue warnings to a data controller/processor that the intended processing is likely to result in infringement of the GDPR;
- Issue reprimands to a data controller/processor where processing operations have infringed provisions of the GDPR;
- Order a data controller/processor to bring processing operations into compliance (with specific direction and time period if appropriate);
- Order a data controller to communicate a personal data breach to an individual;
- Impose a temporary or definitive limitation including a ban on processing;
- Order the rectification, restriction or erasure of data or order a certification body not to issue a certificate;
- Impose administrative fines; and
- Order the suspension of data flows to a recipient in a third country or to an international organisation.

### Application and setting of the fines

The Article 29 Working Party has issued guidelines on fines. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

**Guidelines on the application and setting of administrative fines WP 253, of 3 October 2017**

Once an infringement of the Regulation has been established, the competent DPA must identify measure(s) most appropriately addressing the infringement.

According to the guidelines, when applying the corrective powers, the DPA must observe the following principles:

***Infringement should lead to the imposition of "equivalent sanctions".***

*The DPAs should avoid differing corrective measures in similar cases.*

***Like all corrective measures chosen by the DPAs administrative fines should be effective, proportionate and dissuasive.***

*The assessment of what is effective, proportional and dissuasive will have to reflect the objective pursued by the corrective measure chosen, that is either to re-establish compliance with the rules, or to punish unlawful behaviour (or both).*

***The DPAs will make an assessment in each individual case.***

*The DPAs are encouraged to use a considered and balanced approach when imposing corrective measures in order to achieve an effective and dissuasive as well as a proportionate effect. The point is neither to treat the fines as a last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool.*

***A harmonized approach to fines requires active participation and information exchange among the DPAs.***

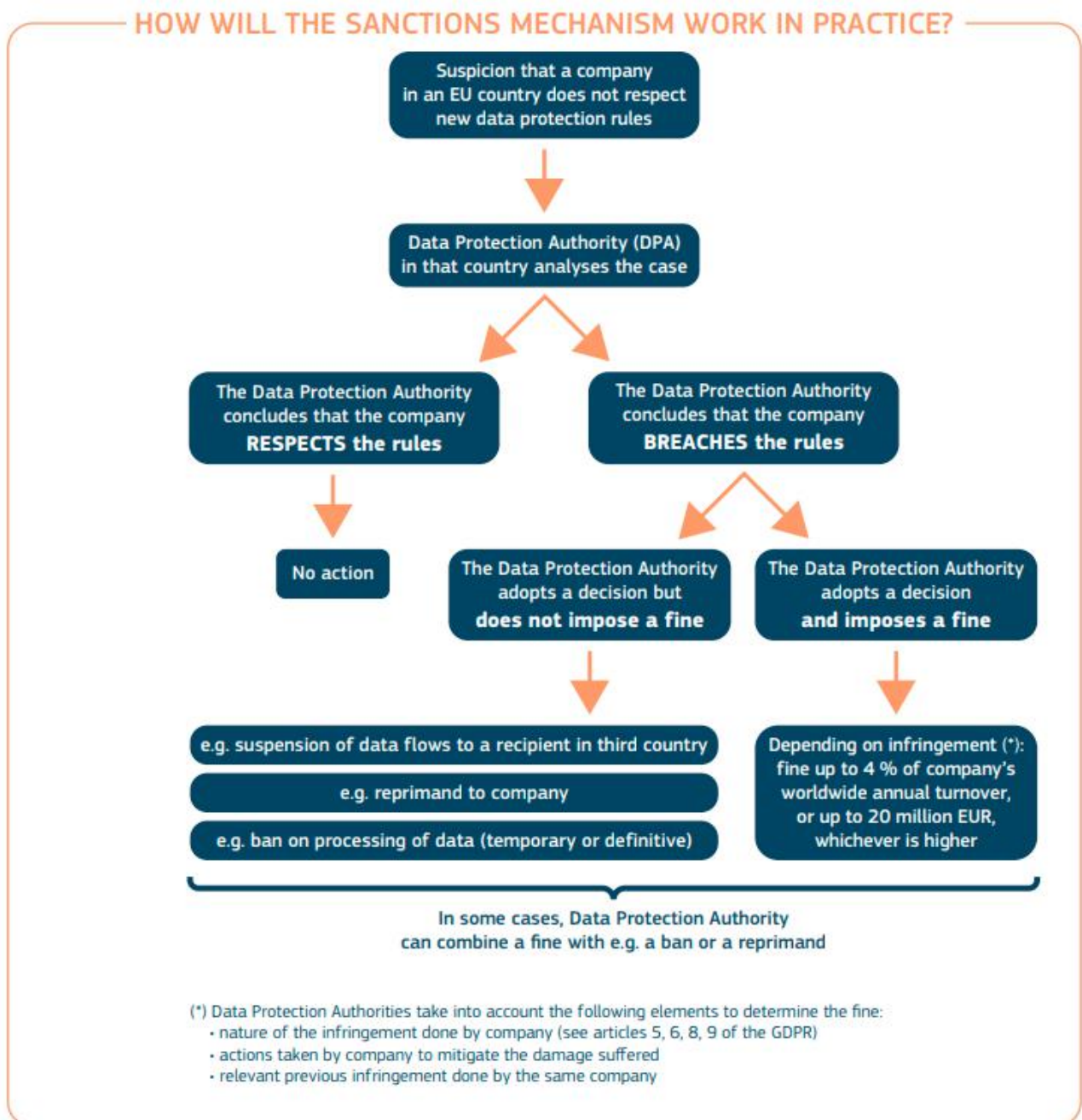
*This means that the DPAs shall cooperate with each other and, where required, with the European Commission*



## Factors for the DPAs to consider when imposing a fine

Having established a violation, the DPA does not always have to impose a fine.

Instead of a fine, the DPA may impose other measures, for example use a reprimand in the case of a minor infringement or where the data controller is a natural person and the fine would impose a disproportionate burden.



According to the guidelines, the DPAs shall consider the following criteria when deciding whether to impose an administrative fine and indetermining the amount of such fine in each individual case.

### 1. The nature, gravity and duration of the infringement

Several different infringements committed together in a single case means that the DPA can impose the fine at the level of the gravest infringement as a limit.

The **nature and gravity** should be assessed given factors such as:

- The number of affected individuals to identify whether this is an isolated event or a systematic breach or lack of adequate procedures.
- The purpose of the processing.
- If the individuals have suffered damages, the level of the damages to the rights and freedoms of the individuals.

**Duration** may be assessed given:

- Wilful conduct by the data controller;
- Failure to take appropriate preventive measures;
- Failure to put in place the required technical and organizational measures.

### 2. Intentional or negligent character of the infringement

In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence.

- An intentional breach might be, for example, action explicitly authorized by top management, or data processing contrary to advice from the DPO.
- A negligent breach might be, for example, a failure to comply with the policies, human error, failure to check for personal data in published information, failure to apply technical updates in a timely manner, failure to adopt policies.

### 3. Action taken to mitigate the damage to the individuals

Mitigating actions are important to fine-tune the amount of a fine to the specific case.

For example, data controllers and data processors have an obligation to implement appropriate security measure to prevent data breaches. However, when a breach occurs, the data controller or processor should do all that is possible to limit the consequences of the damage.

### 4. Technical and organizational measures implementing the data protection by design or by default principles

Any applicable "best practice" procedures, industry standards and codes of conduct should be considered.

### 5. Previous infringements

The DPA will look at whether the data controller or the processor have committed the same infringement before.

### 6. Cooperation with the DPA to remedy the infringement

The DPA may also consider whether the behaviour of the controller produced negative consequences to, or had a limited impact on, the rights of the individuals.

### 7. Categories of personal data affected

The DPA shall assess if sensitive data or data relating to criminal convictions have been affected and how such data had been protected, e.g. via encryption.

### 8. Manner of notifying the infringement

An additional factor is how the DPA has been made aware of the infringement: directly by the data controller or indirectly via investigation, complaints, press articles, anonymous tips.

### 9. Previous orders against the controller/processor regarding the same subject-matter

The DPA will consider prior, extensive contact with the DPO for compliance monitoring following a previous infringement.

### 10. Approved code of conduct or approved certificate mechanism

Where the controller or processor has adhered to an approved code of conduct, the DPA might be satisfied that the code monitoring body takes the appropriate action, for example through monitoring and enforcement. In such case, the DPA might decide not to pursue administrative enforcement measures.

### 11. Other aggravating or mitigation factors

Information about profits gained by a breach may be an important consideration in deciding on the level of the fine.



## Overview of the fines

Fines imposed by DPAs should be effective, proportionate and dissuasive.

The GDPR splits the fines in two groups, depending on the gravity and impact of the underlying violation.

AMOUNT	INFRINGEMENT OF THE RULES CONCERNING
Up to <b>10 000 000 EUR</b> or <b>2%</b> of the total worldwide annual turnover of the preceding financial year, whichever is higher	<ul style="list-style-type: none"> <li>• A child's consent</li> <li>• Identifying an individual</li> <li>• Designating a representative in the EU</li> <li>• Data protection by design/default</li> <li>• Joint controllers</li> <li>• Processing by a data processor</li> <li>• Third party liability</li> <li>• Keeping a record of processing</li> <li>• Co-operation with the DPA</li> <li>• Data security</li> <li>• Notifying/communicating data breach;</li> <li>• Data protection impact assessment</li> <li>• Consultation with the DPA</li> <li>• Appointing a DPO, role of a DPO and DPO tasks</li> <li>• Certification mechanism, obligation of certification bodies, and monitoring bodies</li> </ul>
Up to <b>20 000 000 EUR</b> or <b>4%</b> of the total worldwide annual turnover of the preceding financial year, whichever is higher	<ul style="list-style-type: none"> <li>• The principles of processing</li> <li>• Conditions for lawful processing</li> <li>• Conditions for consent</li> <li>• Conditions for processing sensitive data</li> <li>• Individuals' right</li> <li>• Non-compliance with the DPA order</li> <li>• Failure to provide access to DPA</li> <li>• Transfers outside the EU to non-authorised countries or recipients</li> <li>• Specific rules adopted by the Member States</li> </ul>



## THIS CHAPTER COVERED

### **Data Protection Authorities (DPAs) and One-Stop-Shop**

Companies selling in one member state and only processing personal data of residents of that member state are not likely to notice significant differences in their interactions with the DPA. Companies selling in more than one member state will be primarily subject to the authority of a Lead DPA. Companies should identify this Lead DPA (country where the main establishment of the company is located) and the possible other concerned DPAs.

### **Sanctions**

The Regulation significantly increases the level on sanctions that can be imposed on companies violating the GDPR. The highest sanctions may reach up to 20 000 000 EUR or 4% of the company's total worldwide annual turnover. The likelihood of enforcement action will be greater and enforcement will be more coordinated across the EU.

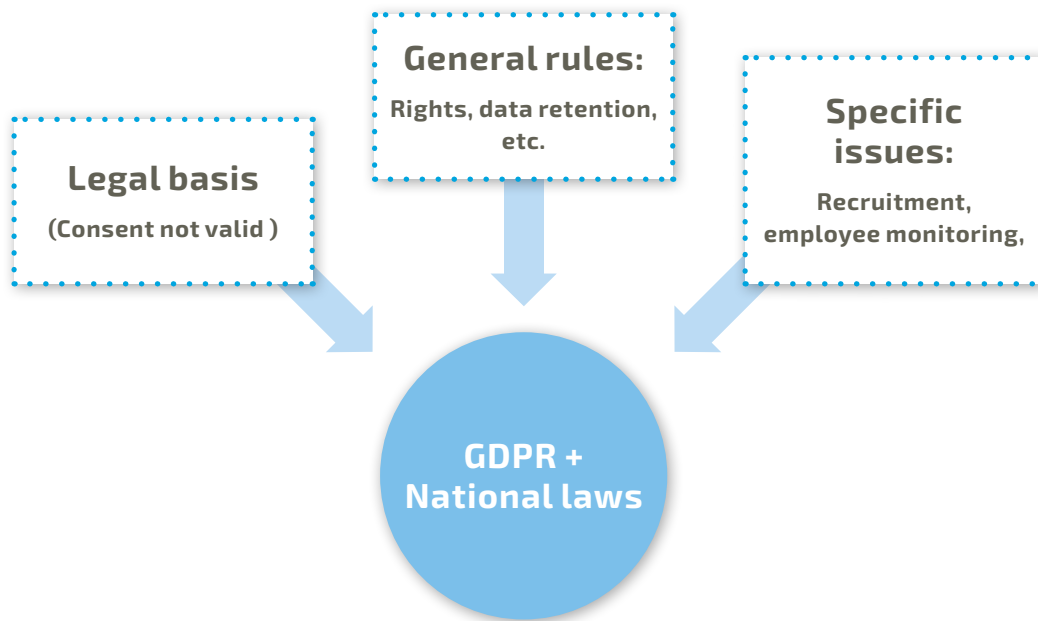
## CHAPTER 9

# PRIVACY IN THE WORKPLACE

---

### 9.1. Privacy in the workplace

ARTICLE 88 OF THE GDPR



**GDPR compliance is not limited to customer data. Each employer has privacy obligations towards their employees. However, as employment laws differ across the EU, the GDPR leaves it to the Member States to adopt specific rules on privacy in the workplace, covering issues like recruitment, performance of the employment contract, diversity, health and safety, etc. Companies will need to comply with national laws concerning privacy in the workplace, in addition to the more generic GDPR obligations.**

Every employer processes personal data of its employees. This includes data sets such as names, address information, contact details, bank account numbers, and salary data, and similar for the purpose of fulfilling the employment contract and managing workforce generally. Employers will also process some sensitive data, such as information about the health of employees or biometric data, for example to manage access to premises.

Data processing also takes place with the employees' every-day use of digital technology and applications provided by the employer (e-mails, calendars, logs). Some employers use monitoring or surveillance technologies, which also amount to personal data processing. This could include: images or video surveillance records, monitoring the use of Internet and e-mail traffic, recordings of phone calls or instant messaging, management of mobile devices, such as phones and laptops, tracking or location data of company cars or equipment.

According to the GDPR, Member States may, by law or collective agreements, provide for specific data protection rules in the employment context. In particular, these rules may be provided for the purposes of:

- Recruitment;
- Performance of the employment contract (including discharge of obligations laid down by law or collective agreements);
- Management, planning and organisation of work;
- Equality and diversity in the workplace;
- Health and safety at work;
- Protection of an employer's or customer's property;
- Exercise and enjoyment (on an individual basis) of rights and benefits related to employment; and
- Termination of the employment relationship.

Any such rules should include suitable and specific measures to safeguard the employees' human dignity, legitimate interests and fundamental rights, with particular regard to:

- The transparency of processing;
- The transfer of personal data within a group company; and
- Monitoring systems at the workplace.

The Article 29 Working Party has issued guidelines on data processing at work. The following comments reflect these guidelines.

*Guidelines from the Article 29 Working Party*

**Opinion 2/2017 on data processing at work, WP 249, adopted on 8 June 2017**

## **Key rules and legal bases for the processing of employee data**

The WP29 has recommended the following key rules to be followed when processing employees' personal data:

### **Legal basis for data processing**

**Consent.** Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences are connected to acceptance or rejection of an offer.

**Performance of a contract.** Employment law may impose legal obligations that require the processing of personal data. In such cases the employee must be clearly and fully informed of such processing.

**Legitimate interest.** Legitimate interest can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity.

The following may be considered as legitimate interests of the employer: detection and prevention of loss of personal data (e.g. customer data), detection and prevention of loss or theft of intellectual or physical business property; and improving employee productivity and performance.

### **Transparency**

Employees must receive privacy information which clearly and fully informs them of the processing of their personal data.

The employer can provide this information in a statement or an internal privacy policy. This policy must be communicated in a clear way and should be easily accessible to employees. Each employee should receive this information. It may be also included in the employee portal, so that it can be accessed and downloaded at any time.

If employee monitoring is involved, the notice should include information about any monitoring that takes place, the purposes for this monitoring and the circumstances, and how they can prevent their data being captured by monitoring technologies. Policies and rules concerning legitimate monitoring must be clear and readily accessible. When creating such rules, the WP29 recommends to involve employee representatives.

### **Rights**

Employees should be given the opportunity to exercise their rights (inspection, correction, erasure and restriction of processing of their data).

### **Proportionality and data minimization**

Data processing at work must be proportionate.

The employer should conduct a proportionality test before deploying any employee monitoring tools. For example if misuse of digital technologies can be prevented (e.g., by using web filters) the employer has no general right to monitor.

A blanket ban on using work equipment for communication for personal reasons is impractical. Enforcing such a ban might require a level of monitoring that may be disproportionate. The information registered from the ongoing monitoring, as well as the information that is shown to the employer, should be minimized as much as possible. Employees should have the possibility to temporarily shut off location tracking, if justified by the circumstances.

Technologies that track vehicles can be designed to register the position data without presenting it to the employer. Data minimisation principles should guide the deployment of new technologies.

### **Data retention**

Data retention periods should be minimized and where information is no longer needed it should be deleted.

## ***Practical examples of privacy and monitoring at work***

WP 29 also provides guidelines for the legitimate use of new technology in a number of specific situations.

### **Social media and recruiting new staff**

An employer can in principle examine the social media profiles of a potential new employee on condition that the social media account is related to professional purposes and where the profile is likely to contain information about skills or characteristics of the candidate, that are directly relevant to the job on offer.

### **Employee monitoring**

Any results of the monitoring of employees must be used solely for the purpose for which they are obtained.

Results of monitoring used to detect and prevent data security breaches, or to detect and prevent fraud, may not be used to assess employees' performance.

Any decisions about the performance of employees, or about the terms of their employment, may never be made solely based on automated processing and monitoring.

Monitoring employees and processing personal information obtained through monitoring is permitted provided the following requirements are met:

- There is a policy that has been communicated and made available to employees.
- This policy clearly describes in which cases monitoring can take place, for what purposes, by whom, how long the data will be stored, and the rights of employees.

- Employees, or their representatives should be actively involved in developing the policy.

Any monitoring, and the processing of resulting information, must not restrict the fundamental right to privacy of employees.

### **Monitoring of communication**

The contents of electronic communications and the traffic data relating to those communications, enjoy the same protection as traditional communications.

The fact that an employer has the ownership of the electronic means does not invalidate the right of employees to secrecy of their communications, related location data and correspondence. The tracking of the location of employees through their self-owned or company-issued devices should be limited to where it is strictly necessary for a legitimate purpose.

In the case where the employees use their own devices for work purposes (Bring Your Own Device), it is important that employees are given the opportunity to shield their private communications from any work-related monitoring.

### **Camera surveillance at work**

An employer needs to determine a legitimate interest for each camera installed. For example, securing business property may be legitimate interest that could outweigh the privacy interest of the employee.

An employer should always consider whether another means with less impact on privacy can achieve the same purpose. For example, a motion sensor, or a camera pointed at the doors rather than at the workspaces of employees.

Employee behaviour should not be continuously recorded. Cameras installed for security purposes may not be used to review employees' general work performance and attendance.

There should be clear rules about how long the recordings are stored, who may review such recordings, and in which cases. Employees should be appropriately informed of this.

Cloud services, online applications and international transfers.

Where employees use online applications which process personal data (such as online office applications), employers should consider enabling employees to designate certain private spaces to which the employer may not gain access under any circumstances, such as a private mail or document folder.

Most applications operating in the cloud involve international transfer of employee data. Employers should ensure that such transfers are in accordance with the data transfer rules and adequate protection is ensured.

### **Biometric data processing**

Member states are permitted to create their own rules concerning biometric data.

Automated monitoring and recognition of employees' facial features and expressions, is generally considered unlawful.

Using biometrics for access control in the workspace, such as facial, iris, or fingerprint scanners, appears problematic as well, as employers cannot rely on consent, and no other exception to the general prohibition of processing biometric data appears applicable.

### **Tracking of vehicles used by the employee**

An employer may want to follow the movement of its transport fleet by installing specific tracking technologies in vehicles. An employer may be able to rely on legitimate interest to recover the vehicle after a theft.

Real-time viewing of location data will usually violate the privacy of the employee who is traveling with it, unless there is a specific incident that can justify this, such as theft of the vehicle, or if the current delivery is running late.

### **Working from home and other forms of remote working**

An employer may rely on legitimate interest to appropriately safeguard the security of sensitive (personal) data processed while working remotely, and to check whether employees working remotely are indeed working the agreed amount of time.

It is not legitimate to use monitoring tools which record keystrokes, screen activity, webcam footage, and/or microphone recordings to keep track of the activities of employees working remotely. The impact of such technologies on privacy is generally too significant to be justified, even if the equipment (laptops, smartphones) is owned by the employer.

If the equipment is not owned by the employer, any monitoring tools installed or used on employee equipment could potentially be classified as a computer crime.

## THIS CHAPTER COVERED



Companies need to carefully assess current employee processing activities and identify what actions will need to be undertaken to comply with the GDPR. Companies should update their existing procedures and implement the changes necessary to comply with the new obligations.





# CHAPTER 10

## ADDITIONAL INFORMATION

### 10.1. Data Protection Checklist

This checklist is aimed to help companies organise their approach to undertaking GDPR compliance. This list is not exhaustive and companies may need to undertake other measures.

COMPLIANCE MEASURE	DESCRIPTION
INITIAL ACTIONS	
<b>Audit</b>  <a href="#">SEE CHAPTER 5 ON ACCOUNTABILITY</a>	<ul style="list-style-type: none"> <li>Do a gap analysis of what procedures are in place for meeting new and existing data protection obligations. Identify any shortfalls and implement a plan to address the gaps.</li> <li>Identify and review all relevant existing internal and public-facing policies and procedures, and identify where data is processed within the company. Remember to look not only at IT, data security, marketing and HR policies but also at third party service providers.</li> <li>Consider if there are existing audit processes which can be leveraged to monitor compliance in this area.</li> </ul>
<b>Internal process</b>  <a href="#">SEE CHAPTER 5 ON ACCOUNTABILITY</a>	<ul style="list-style-type: none"> <li>Identify key internal actors responsible for data processing so that they can be involved in developing new processes.</li> <li>Identify key senior stakeholders to support the accountability programme and the operational (and cultural) changes required to address the accountability requirements.</li> </ul>
<b>Internal policies</b>  <a href="#">SEE CHAPTER 5 ON ACCOUNTABILITY AND CHAPTER 2 ON PRINCIPLES (DATA RETENTION)</a>	<ul style="list-style-type: none"> <li>Create guidelines and policies regarding data retention. There may be specific local requirements, concerning for example employee and medical records.</li> </ul>
<b>Internal process</b>  <a href="#">SEE CHAPTER 5 ON ACCOUNTABILITY</a>	<ul style="list-style-type: none"> <li>Create a new, or update existing, inventory of databases.</li> </ul>

INDIVIDUALS' RIGHTS	
<b>Notice and consent</b>  <a href="#">SEE CHAPTER 2 ON LEGAL BASES FOR PROCESSING AND CHAPTER 2 ON INDIVIDUALS' RIGHTS</a>	<ul style="list-style-type: none"> <li>• Identify and review all existing privacy notices and policies concerning employees and customers. Include all relevant people within the company, legal, compliance, HR, etc.</li> <li>• Review and revise all privacy notices to ensure they comply with the new requirements.</li> <li>• Establish in which countries the notices must be translated.</li> <li>• Establish where you need to obtain consent (explicit and unambiguous).</li> <li>• Decide how privacy notices, policies and consents will be provided and tracked (automated or manual process, etc.).</li> <li>• Look at DPA guidance, as they may provide standard formats for notice.</li> </ul>
<b>Rights</b>  <a href="#">SEE CHAPTER 2 ON INDIVIDUALS' RIGHTS</a>	<ul style="list-style-type: none"> <li>• Ensure that there are policies in place for providing access and correction of personal data and the exercise of other individual rights.</li> <li>• Create FAQs for relevant departments in responding to customers' and employees' questions (about operations concerning the collection and processing of their data).</li> </ul>
ONGOING COMPLIANCE	
<b>Security</b>  <a href="#">SEE CHAPTER 6 ON DATA SECURITY</a>	<ul style="list-style-type: none"> <li>• Review and revise data security policies and procedures to ensure they are up to date and fit for compliance with the GDPR.</li> <li>• Create any new policies that are necessary.</li> <li>• Create a data breach response plan.</li> </ul>
<b>Training for employees with access to personal data</b>  <a href="#">NOT COVERED IN ANY SPECIFIC CHAPTER</a>	<ul style="list-style-type: none"> <li>• Create training for employees who have access to personal data (i.e. HR, IT, finance). Refresh the training, as necessary.</li> <li>• This is not strictly required under the GDPR but is recommended as good practice.</li> </ul>
<b>DPO</b>  <a href="#">SEE CHAPTER 5 ON ACCOUNTABILITY</a>	<ul style="list-style-type: none"> <li>• Establish if you need to appoint a DPO.</li> <li>• Assess whether you should appoint an internal DPO among staff, employ someone new, or hire an external consultant.</li> <li>• Set out in detail tasks and duties of the DPO and include them in the appointment contract.</li> <li>• Create budget to provide resources for the DPO.</li> <li>• Publish contact details of the DPO (privacy policy, website) and communicate them to the relevant DPA.</li> </ul>
<b>Agreements with service providers</b>  <a href="#">SEE CHAPTER 7 ON DATA FLOWS</a>	<ul style="list-style-type: none"> <li>• Identify and audit existing agreements with service providers who act as data processors.</li> <li>• Update and negotiate amendments, to ensure compliance with the GDPR.</li> </ul>

<b>Data Privacy Impact Assessment (DPIA)</b> <a href="#">SEE CHAPTER 5 ON ACCOUNTABILITY</a>	<ul style="list-style-type: none"> <li>• Create DPIA procedure and templates.</li> <li>• Assess where it will be necessary to conduct a PIA. Who will do it? Who needs to be involved? Will the process be run centrally or locally?</li> <li>• Determine whether consultation with a relevant DPA is required following a PIA.</li> </ul>
<b>Codes of conduct and certification</b> <a href="#">SEE CHAPTER 5 ON ACCOUNTABILITY</a>	<ul style="list-style-type: none"> <li>• Consider adhering to codes of conduct and certification mechanisms developed by sector associations.</li> </ul>
<b>Data transfers</b> <a href="#">SEE CHAPTER 7 ON DATA FLOWS</a>	<ul style="list-style-type: none"> <li>• Identify what data flows take place with third countries, and what mechanisms exist for these data transfers and assess their validity under the GDPR.</li> <li>• For intra-group data transfers, consider carrying out a BCR gap analysis to determine the practical viability of BCR.</li> </ul>

## 10.2. GDPR guidelines from Data Protection Authorities

2018

### European Data Protection Board

- [Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679](#),  
25 May 2018
- [Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679](#),  
25 May 2018

### Article 29 Data Protection Working Party

- [Guidelines on Consent under Regulation 2016/679\(wp259rev.01\)](#),  
16 April 2018
- [Guidelines on Transparency under Regulation 2016/679 \(wp260rev.01\)](#),  
11 April 2018
- [Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU](#),  
11 April 2018
- [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679: WP 251](#),  
6 February 2018
- [Guidelines on Personal data breach notification under Regulation 2016/679: WP 250](#),  
6 February 2018

2017

- [Guidelines on transparency under Regulation 2016/679: WP 260](#),  
2017
- [Guidelines on Consent under Regulation 2016/679: WP 259](#),  
28 November 2017
- [Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules: WP 256](#),  
29 November 2017
- [Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules: WP 257](#),  
29 November 2017
- [Working document on Adequacy Referential \(update of Chapter One of WP12\): WP 254](#),  
28 November 2017
- [Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679: WP 253](#),  
3 October 2017
- [Opinion 2/2017 on data processing at work: WP 249](#),  
8 June 2017
- [Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679: WP 248](#),  
4 April 2017
- [Guidelines for identifying a controller or processor’s lead supervisory authority: WP 244](#),  
5 April 2017
- [Guidelines on Data Protection Officers \(‘DPOs’\): WP 243](#),  
5 April 2017

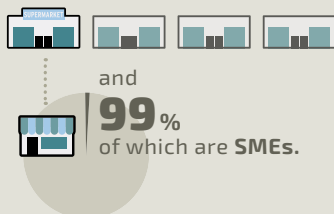
## 2016

- [EU-US Privacy Shield F.A.Q. for European Individuals: WP 246,](#)  
13 December 2016
- [EU-US Privacy Shield - F.A.Q. for European Businesses: WP 245,](#)  
13 December 2016
- [Guidelines on the right to data portability: WP 242,](#)  
5 April 2017



EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 31 countries and 5.4 million companies, both leading multinational retailers such as Carrefour, Ikea, Metro and Tesco, and many small family operations. Retail and wholesale provide a link between producers and 500 million European consumers over a billion times a day. It generates 1 in 7 jobs, providing a varied career for 29 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognised European social partner for the retail and wholesale sector.

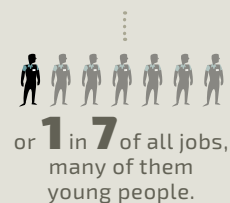
**1 in 4** companies  
in the EU



**10%** of EU's GDP



**29** million jobs



[www.eurocommerce.eu](http://www.eurocommerce.eu)

Follow us on



January 2019