

THE NEW EU DATA PROTECTION RULES

A GUIDE FOR RETAILERS



This guide was written by Joanna Lopatowska, adviser on 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 will need to address between now and 2018, when it comes into force.

Foreword

I am pleased to present this guide, which is aimed at offering an analysis and basic information about the 2016 General Data Protection Regulation, and providing some help to retailers in how to comply with the Regulation when it comes into force in 2018.

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 10 years ago. In equal measure, the dangers of data being compromised, 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 new 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. One point that goes without saying – the earlier companies prepare for complying with the new rules, whether in dealing with data on customers or on their staff, the better they will be equipped to deal with the changes that the Regulation brings with it.



Christian Verschueren
Director-General

Abbreviations and symbols used in this guide

Directive

Data Protection Directive 95/46/EC

DPA

Data Protection Authority / Supervisory authority

DPO

Data Protection Officer

EU

European Union

The Data Protection Directive and the GDPR are both applicable in the European Economic Area (EEA), which comprises 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



EuroCommerce comments on specific rules and requirements (in italic and blue).

The comments and examples provided are non-exhaustive.

Regulatory guidance issued after the publication of this guide may provide additional examples, but also possibly interpretation of the GDPR.

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. 10 key steps to compliance	9
What is the GDPR and why is it relevant for retailers?	11
.....	
1. Getting familiar with data protection	13
1.1. When and why retailers use personal data	13
1.2. Examples of personal data typically processed by retailers	14
1.3. Personal data and other key concepts	15
1.4. Which companies must comply with the GDPR?	17
1.5. Current EU data protection laws	20
.....	
2. General rules	23
2.1. Data protection principles	23
2.2. Key information about privacy notices	25
2.3. Legal basis. When can companies process personal data?	29
.....	
3. Customer privacy	33
3.1. Selected consumer privacy issues relevant for retailers	33
.....	
4. Individuals' rights	39
4.1. Key individuals' rights concerning their personal data	39
4.2. Redress and legal claims	42
.....	
5. Accountability	45
5.1. Key accountability requirements	45
5.2. Data Protection Officer (DPO)	49

6. Data security	53
6.1. Basic information about data security	53
6.2. Personal data breaches	56
6.3. Cybersecurity	59
7. Data outsourcing and offshoring	61
7.1. Engaging service providers	61
7.2. Basic principles on transferring personal data outside the EEA	63
7.3. Selected data transfer mechanisms	66
8. Enforcement	69
8.1. Data Protection Authorities (DPAs) and One-Stop-Shop	69
8.2. Sanctions	70
9. Privacy in the workplace and other issues regulated nationally	73
9.1. Privacy in the workplace	73
9.2. Examples of where member states may adopt specific national laws	75
10. Data protection checklist	77

EXECUTIVE SUMMARY

10 key steps to compliance

1. Getting familiar with data protection

Companies should get to know, and be comfortable with, general data protection concepts and understand the role of their company as primarily responsible for the fairness, legality and security of the processing of personal data.

This concerns both big and small retailers, selling online 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. General rules on transparency 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 have provided privacy notices under the Data Protection Directive should review them and 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 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 data.

Many of these issues are currently unclear. What is clear is that, under the GDPR, retailers will need to explain, in a much clearer and accessible way, how they and their business partners are using 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. Awareness of the changes that are coming should be raised internally. Key management should be on board with changes, so that additional budget expenditure can be planned. Implementing the GDPR might be costly.

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 will also require creating procedures for data privacy impact assessment (PIA) to review any risky processing and steps to address any concerns. Knowing any relevant local law and guidance will be necessary for companies operating in more than one member state.

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. This agreement may be affected by the change of administration in the U.S. in 2017.

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. Local compliance

Companies operating in different member states should determine if there are any specific local rules concerning personal data, in particular in the field of employment.

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 have to tailor the necessary 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 and employees 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, employees' bank account number to pay salaries, 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.

These responsibilities will now be added to. The newly adopted 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 EEA.

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, until now, companies have not implemented robust privacy standards they will have to do it under the GDPR. This may require additional resources and a new way of doing things.

The GDPR takes full legal effect and will be enforced as of 25 May 2018.

Before the Regulation takes full legal effect in May 2018, companies will have almost two years to implement necessary changes. While this may seem a long way away, companies should act now, as many of the obligations will take time to integrate. Being proactive about the GDPR can help save time and money.

In this guide, we outline some of the key areas in which the retailers operating in the EEA 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 EEA in most areas, but member states have retained competence to adopt specific privacy rules in some areas.

NEW OBLIGATIONS. DPO, Privacy Impact Assessment (PIA), breach notification, documentation, privacy by design and default, new privacy notice requirements.

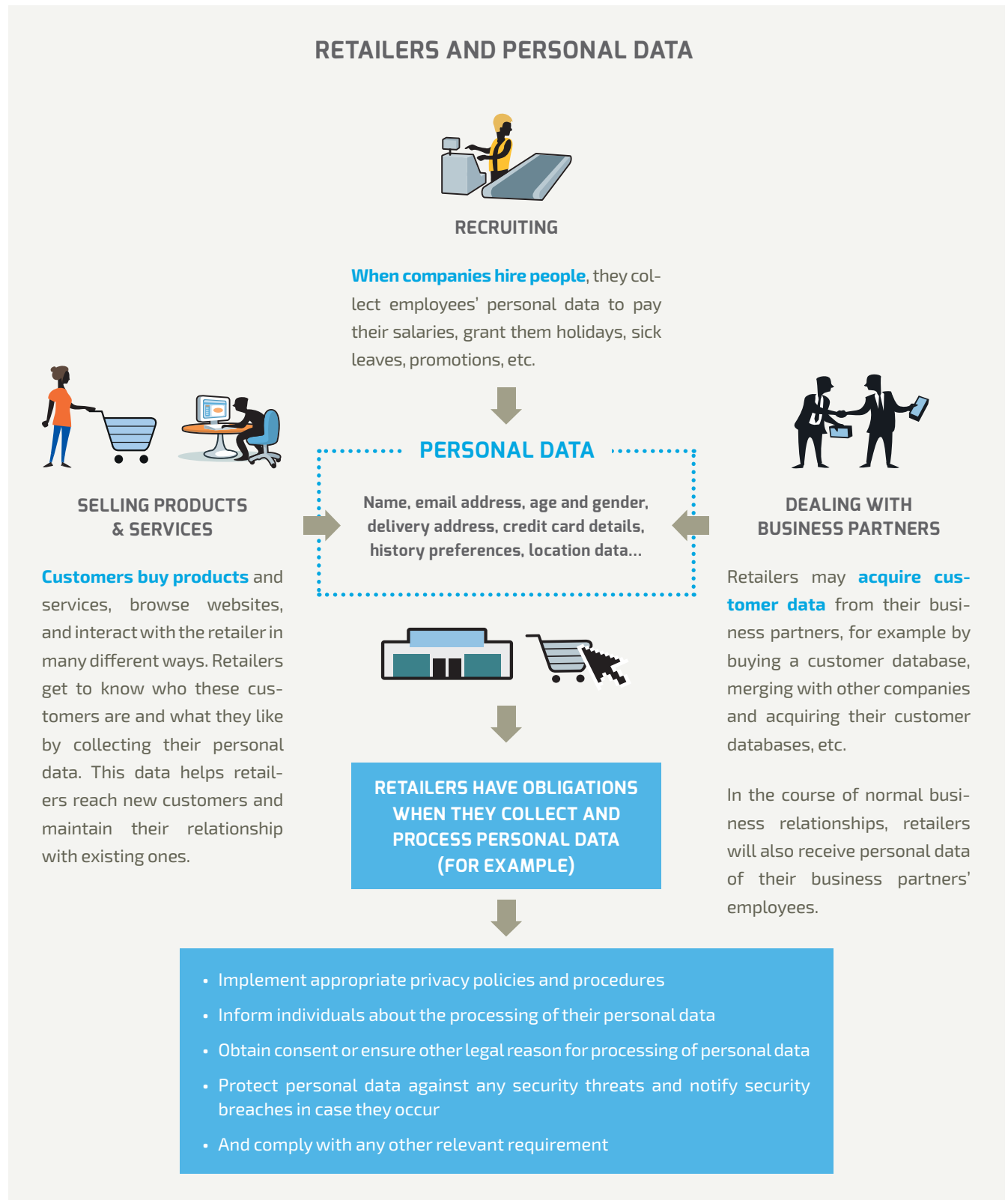
HIGH FINES FOR VIOLATIONS. Sanctions up to 20 million EUR or 4% of global annual turnover.

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, complaints.

Support inquiries: telephone numbers and duration of any calls requesting support, subject 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.

The Regulation expressly considers as online identifiers a name, an identification number, location data, online identifier or other factors related with the physical, physiological, genetic, mental, economic, cultural or social identity of a person. Technology-based identifiers such as MAC addresses qualify as personal data.

Employee personal data

Personal details: name, contact details (email, phone numbers, physical 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/re-hire and termination date(s) and reason, length of service, 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.

1.3. Personal data and other key concepts

ARTICLE 2 OF THE GDPR

In order to comply with their obligations under the GDPR, companies have to 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.

In this guide we have replaced the term "data subject" with "individual."



Often, a single piece of information such as gender or postal code cannot be used to identify an individual. However, such information in combination with other data can. For example, one study found that 87% of Americans can be uniquely identified by combining three indirect identifiers: date of birth, gender and postal code. With the development of the computing technologies, less and less information is needed to identify an individual. Therefore, information that may appear to be not personal may turn out to be personal data.

Data controller

The individual or organization, 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
- Asking customers to provide their address in order to deliver goods bought online
- Analysing customers' shopping preferences via their use of loyalty cards
- 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' 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
- 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 controller.



A data processor can be:

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

DPA


A national supervisory data protection authority, an independent authority tasked with supervising and enforcement of data protection rules.

Consent

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


Profiling

Any form of automated processing of personal data consisting of 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 sophisticated tools to collect and analyse such data in order to reach consumers faster and more effectively by providing more 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.

Pseudonymisation

The processing of personal data in such a way that the data can no longer be attributed to a specific 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. Pseudonymous data is still regarded as 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.

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 the 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.

Sensitive data

Any data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life.

 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. Biometric data is also defined but is not considered to be sensitive data. Retailers may be using biometric data, for example for managing employee working time, allowing access to secure areas. The processing of biometric data may require a data protection impact assessment.

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

GDPR applies to companies established in the EEA and outside the EEA

The existing **Data Protection Directive** applies to any company established in the EEA. However, only data controllers have direct obligations. Companies established outside the EEA must comply with the EEA privacy rules if they use "means of processing" located in the EEA to process personal data which means equipment, such as servers, located in the EEA or using a service provider located in the EU for the processing of personal data.

Companies established in the EEA

According to the **GDPR** any company (data controller and data processor) established in the EEA must comply with the EU privacy rules irrespective of where the personal data is located or where the processing takes place. There are no big changes; these rules already apply under the Directive.

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



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

Companies established outside the EEA

The GDPR applies to any company (data controller or data processor) established outside the EEA, if that company:

- Offers goods or services to EEA residents; or
- Monitors the behaviour of EEA residents (such as profiles or tracks them online).

These are big changes. Currently many companies established outside the EEA that collect Europeans' personal data do not have to comply with the Directive, but many of these companies will have to comply with the GDPR once it comes into force.



Many online businesses that make their websites available in the EEA and target individuals in the EEA will be covered by the Regulation. Targeting individuals means for example, language used on a website or advertisement directed at residents of certain countries, or the acceptance of local currency with the possibility of ordering goods and services in that language (Recital 23). For example, a U.S. retail chain that markets its products directly to EEA residents, but has no physical presence in the EEA, is not covered by the Directive, but will need to comply with the GDPR. A company whose website is accessible to EEA consumers will not automatically be covered by the Regulation if it is not actively targeting Europeans.

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

The GDPR sets out privacy rules that must be followed by all companies operating in the EEA, irrespective of the company's size, turnover and business model.

The size of a company does not matter. Generally, apart for the record-keeping (documentation) obligation, the GDPR does not include any specific exemptions for the SMEs with fewer than 250 employees.

However, the GDPR encourages the EU institutions, the member states and the DPAs to take account of the specific needs of micro, small and medium-sized enterprises in the application of the Regulation. It is yet unclear what it will mean in practice for the SMEs.

It matters for the compliance with the GDPR how much personal data a company processes and for which purposes, how much risks for the individuals are related to data processing, whether the company operates in one or several countries.

In practice, large retailers will have different compliance measures and priorities they will need to undertake compared to smaller shops.

Measures to ensure compliance with the GDPR will differ, depending on what sort of business is involved:

- **Small bricks & mortar shops** (corner shops, butchers, bakers, fast food shops, boutiques, hardware DIY stores, pet shops, card shops, etc.);
- **SME retailers selling domestically online and in a bricks & mortar** (mainly food shops);
- **SME retailers selling online across the EU and sometimes beyond** (retailers selling clothes, accessories, furniture, homeware, electronics, or sport goods);
- **Large retailers selling online and offline across the EU and beyond** (multinational retailers selling clothes, accessories, furniture, homeware, electronics, or sport goods in most countries in the EU and often having subsidiaries outside the EU).

Suggested steps that small and large retailers may take for basic GDPR compliance



SMALL SHOPS



1. Audit systems to identify what personal data are being collected and for which purposes.
2. Identify risks that may be involved in the processing of personal data by the company: large or small number of customers, customer tracking and profiling, data security risks, collection of sensitive data, etc.
3. Assign data protection oversight function to one of the employees.
4. Ensure that personal data are secure and protected against security risks (IT and physical security).
5. Establish or review necessary privacy policies and procedures.
6. Provide privacy notices to relevant customers and employees.
7. Take any other relevant privacy measure appropriate to the risks involved.



BIG SHOPS



1. Audit systems to identify what personal data are being collected and for which purposes.
2. Identify risks that may be involved in the processing of personal data by the company: large or small number of customers, customer tracking and profiling, data security risks, collection of sensitive data, etc.
3. Review and revise necessary privacy policies and procedures.
4. Ensure robust data security and create a data breach response plan.
5. Roll out or update privacy notice for customers and employees.
6. Create Privacy Impact Assessment procedures and templates.
7. Create or update existing database inventory.
8. Ensure process for exercising individuals' rights.
9. Appoint a DPO, if necessary.
10. Organise regular privacy trainings for relevant employees.
11. Update existing service provider agreements and apply new standards to new deals.
12. If you transfer personal data outside the EU, ensure you rely on appropriate safeguards.
8. Consider certification with privacy certification bodies or adhere to a relevant code of conduct.
9. Take any other relevant privacy measure appropriate to the risks involved.

1.5. Current EU data protection laws

EU data protection rules apply in the 31 member states of the European Economic Area (EEA), which includes the 28 member states of the European Union (EU), Norway, Liechtenstein and Iceland. All the other European countries, and even some beyond, have adopted EU-style data protection laws. Here are the main data protection rules in the EU:

LAW	BRIEF DESCRIPTION	HARMONISATION	STATUS
Data Protection Directive 95/46/EC	Regulates the processing of personal data within the EEA and includes data protection rules on all general aspects of privacy such as principles, collection and use of personal data, etc.	<ul style="list-style-type: none"> • Minimum • Implementation and enforcement vary across the EEA, which means there is a patchwork of 31 data protection laws. 	<ul style="list-style-type: none"> • Currently in place • Will be replaced by the GDPR on 25 May 2018.
General Data Protection Regulation (GDPR) (EU) 2016/679	<p>Regulates the processing of personal data within the EEA and includes data protection rules on all general aspects of privacy such as principles, collection and use of personal data, etc.</p> <p>Compared with the Directive the GDPR boosts individuals' privacy rights and increases companies' obligations.</p>	<ul style="list-style-type: none"> • Full • Member states will keep competence to adopt data protection rules in some areas. • Direct effect – no need for national implementing. 	<ul style="list-style-type: none"> • Will replace the Directive on 25 May 2018.
ePrivacy Directive 2002/58/EC	Regulates privacy in electronic communication such as cookies, spam, data retention, data breaches. Mainly covers telecoms sector.	<ul style="list-style-type: none"> • Minimum • Implementation and enforcement vary across the EEA, which means there is a patchwork of 31 data protection laws. 	<ul style="list-style-type: none"> • Currently in place but is under legal review. • New rules to be proposed by the end of 2016.
Network and Information Security (Cybersecurity) Directive (EU) 2016/1148	Regulates member states' and some types of companies' cybersecurity obligations.	<ul style="list-style-type: none"> • Minimum • The Directive will need to be implemented in national law. • Laws will vary across the EEA. 	<ul style="list-style-type: none"> • Will apply as of 10 May 2018.



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 • Privacy notice • Legality

2.1. Data protection principles

ARTICLE 5 OF THE GDPR

The data protection principles serve to guide the application and interpretation of the GDPR. The application of many concepts and rules in the Regulation are designed to take account of further IT developments to avoid the Regulation becoming quickly outdated. The principles aim to adjust the Regulation to changing technology.

The principles in the current **Data Protection Directive** include fairness, lawfulness, transparency, purpose limitation, data minimisation, data quality, security, integrity and confidentiality.

These existing principles have been kept and strengthened under the **GDPR**. A new accountability principle has been added to require companies to demonstrate compliance with the data protection principles. The principles under the GDPR include.

1. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to an individual. The transparency principle requires operators to inform individuals about what a company does with their personal data.



A company must have a lawful reason to process personal data. Otherwise, it will be breaching the law. For example:

- **Consent:** an individual has consented to the processing of his or her personal data (for example for the purpose of profiling).
- **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 obligations (provide information about employees' salaries to tax authorities).

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.



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 that have been communicated to individuals. The data cannot be shared with marketing partners unless the contest participants have been informed of this.

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.



Only 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. Details such as age, marital status or children are not likely to be necessary to sell goods or ship a parcel.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Companies should take reasonable steps to ensure that personal data that are inaccurate are erased or rectified immediately.



For example, employee payroll records should be updated when there is a pay rise; customers' database should be updated if there were changes in the shipping addresses, or customers have requested to be removed from the mailing list.

5. Storage limitation

Personal data must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed.



Personal data should be depersonalised where possible.

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. Appropriate technical or organisational measures must be used.



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

7. Accountability

The company is responsible for demonstrating compliance with these principles.



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. Key information about privacy notices

ARTICLE 13-14 OF THE GDPR

The GDPR requires any company that collects and processes personal data to inform individuals about it and provide certain information, such as who the company is, why it collects personal data, whether the company shares personal data with any other parties, for how long it keeps personal data, and may other details. Most consumers will never read a privacy notice. They will often agree to give their personal data without reading what they consent to. Their main interest is to buy and receive the goods or a service. People will usually read a privacy notice or complain about how a company handles their personal data when they feel their data have been misused.

The current **Data Protection Directive** requires providing certain information to individuals, including: company's name, reasons for the processing of the individual's personal data, with whom personal data are being shared, that the individuals have the right to access and correct their personal data and any other information necessary to guarantee fair processing. The member states may require companies to provide additional information. Therefore, companies that sell in several member states must comply with a plethora of specific requirements in each country where they sell. This means that companies might need to have different privacy notices and policies in different countries.

The **General Data Protection Regulation** sets a higher standard by adding more information that must be provided to individuals, in addition to the information already required under the Directive. The privacy notices will have to be more detailed. This will impose additional burdens on many companies. However, member states will not be able to set additional requirements. A single privacy notice will be sufficient across the EEA. Companies selling in several member states will not need to adapt the notice to local legal requirements. However, the notice will still need to be translated into the local languages if needed.

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

Generally yes. Privacy policy is a form of a privacy notice. Privacy notice is a general term used to describe information to individuals about the processing of their personal data. It can be short or long, very detailed and comprehensive or focus on one specific aspect of data processing. The term "privacy policy" is generally used for longer documents available on the website or contracts that generally describe company's approach to privacy.

When do companies need to provide a privacy notice?

The purposes for which personal data are processed differ for a customer visiting a website, a job applicant, customer using a loyalty card, or participants in a promotional contest.

A privacy notice will be needed when:

- Collecting information about customers from their loyalty card transactions;
- Selling online and collecting personal data for any purpose: processing the order, shipping the good, customising shopping experience;
- Sending marketing communication;
- Organising contests and collecting email addresses or phone numbers, and any other personal data;
- Analysing customers' shopping behaviour, preferences and likes;
- Collecting job applications;
- Keeping a record of the calls that customers make to call centre;
- Managing employees' personal data to pay salaries, track holidays and sick leave;
- Collecting and processing personal data for any other purpose.

Because data is used for all these different purposes, retailers may need to have different privacy notices for each.

If a company has provided a privacy notice (a general privacy policy or a specific privacy notice) it may need to be updated when personal data are used for a new purpose.



For example, launching a new project, a contest, or a new IT system that changes the way personal data are used and shared will require a new or updated privacy notice.

How to write a privacy notice

The GDPR requires a privacy notice to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child (Article 12.1). Individuals to whom the notice is addressed should be able to understand it.

Here are some suggestions to consider when providing a privacy notice.

- Use **simple and clear language**. Avoid complicated legalese. Use words and titles that people understand.
- Use **appropriate font style and size**. Do not use small print, closely spaced text, small italic font, or grey font, etc.
- Provide **clear and easy-to-find information** on how individuals can obtain more details, and whom they can contact for any questions.
- Provide any necessary information to allow individuals to understand what they are consenting to.
- If **explicit consent** is required (for example for profiling or processing sensitive data) provide an easy way to express consent, such as a clearly visible consent box. The box must not be pre-ticked.
- If **unambiguous consent** is required (in most situations) draft the consent form in a simple and clear language and place it prominently in the privacy notice or in a separate statement.
- Use a **layered privacy notice** for complicated and lengthy information. A layered notice usually includes a short and long text. The short notice available on the front page should usually include basic information about the identity of the company, the purpose of processing and a link to a long notice that explains all the details. A layered notice may be particularly useful to provide on mobile devices.

Things to remember when providing a privacy notice

Under the GDPR, a privacy notice should be provided to all individuals whose personal data are being processed. In the retail context, this generally means to employees and customers. Companies may need to use different channels to communicate the notice to different groups of individuals.

In order to ensure compliance with the new requirements in the GDPR, companies should review all the privacy notice templates provided so far. Companies may need to create new forms.

Privacy notice to employees

Companies should review privacy notices provided to employees in all countries and revise the notices, if necessary, to ensure that they comply with the new rules. This should cover employees, non-payrolled contractors or consultants, agency-supplied contractors or consultants, etc.

New employees should receive the notice at the start of their employment. Existing employees should receive a copy of the updated notice on paper, on the intranet site, or in any other appropriate way.

Where necessary, consent should be collected from the employees. However, under the GDPR, employers will not be able to rely on consent for most types of data processing.

HR managers should be aware of the obligation to provide the notice, obtain consent, know where to access it or obtain further information, or handle a privacy complaint.

Privacy notice to customers

Companies should review privacy notices provided to customers in all countries online and offline, including privacy policies available on website(s), loyalty cards, special bonus programmes, contests, etc. Where necessary, notices should be revised to ensure that they comply with the new rules.

Where cookies or other technologies gathering online data are used for purposes other than those necessary to interact with the website, e.g., for tracking online behaviour for marketing purposes, companies should consider using a pop-up, floater, landing site or similar technology to notify users about the tracking.

A PRIVACY NOTICE CAN BE PROVIDED IN MANY WAYS



In writing: In printed forms (for example in printed materials when providing loyalty card, in printed adverts, on job application forms, etc.)

Electronically: On the website, in text messages, in emails, in apps, etc.



Orally: When speaking to customers on the phone. It is a good practice to document that the notice has been provided.

In combination with standardised **icons** in an easily visible, intelligible and legible way. When icons are presented electronically, they must be machine-readable.



REQUIREMENTS FOR A PRIVACY NOTICE UNDER THE GDPR

<p><i>General</i></p>	<p>A privacy notice (privacy policy) must:</p> <ul style="list-style-type: none"> • Be transparent and easily accessible, • Provide information in an intelligible form, using clear and plain language, adapted to the individual (particularly if it concerns children).
<p><i>Information to be included in a privacy notice</i></p> <p><small>(INFORMATION ALREADY REQUIRED UNDER THE DATA PROTECTION DIRECTIVE PRINTED IN BOLD)</small></p>	<ul style="list-style-type: none"> • Company's name and contact details and the identity and contact details of the DPO (if appointed), • The purposes for the processing of the personal data and the legal basis of doing so, • Information about the individuals' rights, such as: the right of access and rectification or erasure of personal data, restriction of processing, right to object to processing and the right to data portability, • With whom the data are being shared (<i>for example, payment providers, delivery companies, banks, marketing partners, etc.</i>), • If the data processing is based on the legitimate interests, explanation of these interests, • Whether individuals are being profiled, • Information on whether personal data is transferred outside the EEA, • For how long personal data are retained, • The right to withdraw consent at any time, • The right to lodge a complaint to the DPA, • If the processing is based on a contract, the relevant terms of that contract, <p>If the personal data have not been collected directly from the individual, the privacy notice must also state:</p> <ul style="list-style-type: none"> • The categories of personal data concerned, • The source from which personal data have been obtained.
<p><i>Timing</i></p>	<p>Where personal data are collected from an individual, a privacy notice should be provided at the time where personal data are collected. Where data are not collected from the individual (<i>for example when a company bought a customer database</i>), it should provide a privacy notice:</p> <ul style="list-style-type: none"> • Within a reasonable period after obtaining the personal data, but at the latest within one month, or • If the personal data are to be used for communication with the individual, at the latest at the time of the first communication, or • If personal data will be shared with further recipients, at the latest when the data are first disclosed.
<p><i>Exemptions</i></p>	<p>If the personal data are not collected from the individual, a privacy notice is NOT required if:</p> <ul style="list-style-type: none"> • The individual already has the information from another source, • Providing the notice would be impossible or would involve disproportionate effort, • Processing of personal data is governed by specific provisions or personal data is confidential.

2.3. Legal basis. When can companies process personal data?

ARTICLE 6-11 OF THE GDPR

Companies can process personal data only if they have a legal basis – a “good reason” – to do so. This is in accordance with the lawfulness principle.

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

Consent

Consent is one of the fundamental concepts of data protection law in the EEA and globally. Consent means that an individual agrees to the collection and the processing of his or her personal data. It is seen as the most transparent way to ensure that the data processing is fair and legal. However, the obligations under the GDPR make consent a less attractive option.

Under the GDPR consent is defined as:

a. Freely given,

b. Specific and informed,

c. An 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 GDPR distinguishes between explicit and unambiguous consent without however strictly defining these terms.

Explicit consent is required for the processing of sensitive data, for profiling and for transferring personal data outside the EU.

For other types of processing, unambiguous consent will suffice.

Consent cannot be relied upon indefinitely - an individual may withdraw consent. If consent is withdrawn, data processing must cease. Therefore, when relying on consent, extra care will be needed to ensure that circumstances have not changed.

Retailers will most likely need to obtain consent when:

- Tracking customers online and analysing their browsing and shopping behaviour for marketing purposes,
- Using data obtained from loyalty cards,
- In some countries sending direct marketing via email, sms (see ePrivacy Directive).

Consent will not be necessary in order to process a transaction, for example, to sell online and send parcels to consumers.

a. Freely given consent means that an individual must have a “genuine and free choice”. For example, performance of a contract or provision of a service must not be made conditional on the 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 provided through an action like clicking a button or link, it must also be withdrawn through a similarly simple and easily accessible action.

b. Specific and informed means that it must be separated from any other type of consent and action.



For example, agreeing to the terms of service for delivery of an item bought online should be a separate action from agreeing to have personal data shared with third parties for marketing purposes. Being informed also means knowing about all the reasons why personal data is being processed. It also means being informed of the rights and the ability to withdraw consent or object to some types of processing, like profiling.

c. Unambiguous consent provided via affirmative action could include ticking a box when visiting a website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity do not constitute consent.



The requirement for “unambiguous” consent is less onerous than “explicit” consent, but it still depends on a “clear affirmative action”.



Unambiguous consent expressed by affirmative action is more than “implied consent” where simply using a service, particularly a digital one, can be taken as an indication of agreement. Unambiguous consent is likely to require higher standards than implied consent (required for the placing of cookies). The individual must take a clear action, for example clicking a “Continue” button on a web page. Clarification from the DPAs will be needed to understand what concretely companies will need to do to achieve unambiguous consent.

Parental permission is required to process the personal data of children. A child is considered to be anyone under the age of 16.

One of the conditions for valid consent is that the company must demonstrate that consent was given by the individual. Failure to keep such a proof of consent will be a breach of the rules. This means not just recording the fact that someone ticked a box in a form, but having an audit that links the action to any privacy notice and the actual processing of the data concerned.

Legitimate interest

This legal basis allows companies to process personal data without consent when companies need personal data for their own legitimate interests (such as commercial, marketing purposes). However, legitimate interest must be balanced with the rights and freedoms or legitimate interests of the individual whose personal data is being processed.

According to the GDPR, processing is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal data, in particular where the individual is a child.

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 at the time and in the context of the collection of the personal data that processing for that purpose may take place.

Such legitimate interest could exist where there is a relationship between the individual and the company, such as the individual is a client of the company.

Under the GDPR legitimate interest includes:

- The processing of personal data is for **direct marketing** purposes. (Recital 47)
- The processing of personal data is strictly necessary for the purposes of preventing **fraud**, for example internal compliance programmes. (Recital 47)
- Personal data are 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)
- The data processing is strictly necessary and proportionate for the purposes of **ensuring network and information security**. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping “denial of service” attacks and damage to computer and electronic communication systems (Recital 49)

Balance between the company's legitimate interest and individuals' rights

The legitimate interest requires a balancing of the legitimate interests of the company against the interests and fundamental rights of the individual. To determine this balance, a number of factors will need to be considered:

- The nature and source of the legitimate interest, whether the relevant processing activity is necessary for the exercise of a fundamental right, or is otherwise in the public interest,
- The impact on the individual,
- The individual's reasonable expectations
- The nature of the data and how those data are processed;
- Additional safeguards that the company can implement to limit any undue impact on the individual (e.g., data minimisation, privacy-enhancing technologies, increased transparency, a right to opt-out, and data portability).

Many companies currently rely on a "legitimate interest" as a lawful basis for the processing of personal data. Individuals can always object to the processing of their personal data.

The GDPR reverses the burden of proof. Rather than the individual having to demonstrate justified grounds for objecting, the company must demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual. As a result, many businesses may find that they are no longer able to rely on legitimate interest as a lawful basis for the processing in the course of some of their business activities.

New purposes

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

If personal data are 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 have been collected, including the company's relationship with the individual;
- The nature of personal data, in particular, whether sensitive data are affected;
- The possible consequences of the new purpose;
- The existence of appropriate safeguards (e.g., encryption or pseudonymisation).

The current Data Protection Directive also permits the processing of personal data for new purposes, provided those new purposes are "not incompatible" with the original purpose. The GDPR makes this process more difficult, because it is very burdensome to determine which new processing purposes are "compatible", and which are not.

Contractual necessity

Personal data may be used without consent if this is needed to perform a contract, for example sell and deliver goods.



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. It is not necessary to require consent for processing these data. The processing of personal data may also be required before entering into contract, for example an individual requests information from a retailer about a particular product in order to conclude a contract.

Legal obligation

This legal basis means that there must be an obligation to comply with specific law, which requires a company to collect and process personal data. This does not typically exist in the retailer-consumer relationship but may concern employee relations.



For example, companies need to collect certain employee data in order to comply with tax obligations.



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 make a company more transparent and more accountable and reassure people 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.

Legality

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

CHAPTER 3

CUSTOMER PRIVACY IN THE RETAIL CONTEXT

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

3.1. Selected consumer privacy issues relevant for retailers

Neither the GDPR nor the Data Protection Directive contain any specific rules on the processing of personal data in a sector specific context, such as, for example retail. In addition, privacy rules are designed to be technology neutral. This means that there are no specific rules about using personal data by the retailers and for their commercial purposes, whether online, offline or omni-channel. 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 will need to explain, in a much clearer and accessible way how they and their third party partners are using the consumer information they collect.

Below 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.

Under the current **Data Protection Directive** the individuals have a general right "not to be subject to a decision which produces legal effect concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him." Such automated processing is essentially profiling but there are no specific constraints or obligations linked to it (such as a need for explicit consent); general data protection rules apply.

Under the **Regulation**, individuals should not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (e.g., a bank decides not to grant a mortgage on the basis of profiling information) (Article 22). This is similar to the Directive, but the related obligations are much more stringent.

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 will only be permitted:

- **With the individual's** explicit consent;
- If expressly authorised by EU or member state law; or
- If it is necessary for entering into, or performance of, a contract between the individual and a company.

Profiling is prohibited if it is based on the processing of sensitive personal data.

Companies that profile individuals must inform them upfront about the profiling and in most cases obtain individuals' explicit consent. Companies that regularly rely on data analytics will need to consider how to implement appropriate transparency and consent mechanisms in order to continue profiling activities under the Regulation.

In many situations, the only lawful basis for profiling will be the explicit consent of the individual. This could mean that analytics involving personal data may require explicit consent before the analyses can be conducted, for example in relation to customer tracking, behavioural targeting and advertising.

As the GDPR requires explicit consent, lawful profiling could become much more onerous. In addition, individuals will need to be informed about the profiling and its consequences.

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



Children

Children are exposed to privacy risks when their personal data are 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 commercial value of their personal data. Like most adults, children tend to skip privacy policies and they readily agree to the use of their personal data in order to get access to desired websites.

The GDPR requires parental consent for the processing personal data of children under 16 (Article 8). Children aged 16 or older may give consent for the processing of their personal data themselves.

The age of consent has been set at 16 years, but member states may set a lower age, although not below 13. Differing rules on the age of consent across the EEA could create issues for companies that operate internationally. It is unclear if member states will be consistent on this issue. For example, the UK, has already said that it will lower the age of consent to 13.

Companies will need to start thinking now about putting systems in place to verify individuals' age and to gather parental or guardian consent for the data processing. Companies will be responsible for proving that parental consent has been obtained, which might be particularly difficult in an online context. Therefore, systems should be designed to capture this. A privacy notice concerning children's personal data will have to be written in a way that children understand.



Loyalty cards

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

Currently retailers that offer loyalty cards and programmes must comply with all the relevant data protection rules. They must inform consumers on how they use their personal data, with whom they share the data. They must also keep personal data secure.

The retailers may often rely on their legitimate interests. However, in some situations obtaining consumer consent will be required.

One of the key issues is connecting data from consumers' social media activity and their online and offline transactions, which often involve loyalty cards.

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

Consumers will most likely need to provide explicit consent before the data can be collected, as loyalty programmes are likely to result in customer profiling. However, further guidance from the DPAs will be needed to explain this. Given the particular emphasis on profiling, loyalty programmes may need to differentiate between general consent and consent for personalised marketing.



Direct marketing and targeted advertising

The Regulation explicitly 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, individuals can at any time object to the processing of their personal data for direct marketing purposes. In such cases, personal data may no longer be processed.

Direct marketing has not been defined under the GDPR. Therefore, companies should give consideration to the precise nature of their marketing activity. It may, for example, mean that a simple mailing covering similar goods and services to existing customers and prospects is completely legitimate without direct consent – but it certainly does not include “profiling” for marketing purposes, which does require consent.

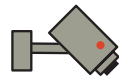


Prize contests

Retailers use prize draws and contests in various forms to promote their commercial offerings. The collection of personal data from contest participants for use in further marketing is often a key element of a promotion.

Currently this is legal and will remain legal under the GDPR, provided the retailer has complied with all the relevant data protection rules, including in particular:

- **Privacy notice.** Companies must have a privacy notice informing participants in a contest about the collection of their personal data via the contest, and for which purposes the retailer will use their data. The policy must be disclosed in an appropriate way to the participants.
- **Consent.** As relying on legitimate interest becomes increasingly more difficult, individual's consent might be required. Companies will need to stay up to date on any relevant regulatory guidance in this regard. If contests are directed at children under 16 parental consent will be required and the retailer will need to prove that such consent has been obtained.



CCTV cameras

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

Companies that operate a surveillance camera in a shop, warehouse, distribution centre, entry hall, car park, or office space, are deemed to be collecting and processing personal data. Images (even if faces are not visible), car number plates can be personal data.

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). In most countries, general data protection rules apply.

The GDPR does not include any specific rules on the capturing and processing of audio-visual images. This means there are no specific rules about the placing of the 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, in particular informing people of the cameras, ensuring data security and allowing access to personal data.



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



Facebook “Like” button

Many retailers include a Facebook “Like” button or other social plugins on their websites.

In recent years having a “Like” button on websites has been questioned by DPAs, including in Belgium and Germany.

This is not a question only for retailers. The “Like” button collects information about a user and shares it with social media, irrespective of whether the consumer is signed up with Facebook or not. Sometimes, information about an individual is transferred to Facebook, without even clicking the “Like” button. Courts have decided that such practice violates the data protection law. For more information see: Düsseldorf District Court, Peek & Cloppenburg case.



It is unclear what measures will need to be undertaken under the GDPR to allow such practices and whether at all such practices will be permitted.



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:

Data Protection Regulation/GDPR: Covers General rules on how personal data are obtained and used, rules on individuals' rights, definition of personal data, consumer profiling, 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 may also apply to other technologies.

The main focus in the e-Privacy Directive is on notice and consent.

Notice: Users must receive clear and comprehensive information (notice) about why cookies are being set. The notice must include what data are collected, for what purpose and with whom they are shared.

Consent: Users must give their consent for information to be stored on or retrieved from their device. Member states have different interpretations of how notice and consent should be delivered, whether it should be opt-in or opt-out, and whether consent obtained through browser settings is valid.

The e-Privacy Directive generally applies to cookies and other tracking technologies (web beacons, advertisement tags). This will cover any information stored on or retrieved from user's device used to track and analyse users' online behaviour, create user profiles, measure online activity, etc.

Information strictly necessary for the operation of a website or its services, information allowing users to better navigate websites and manage their accounts, for example, by storing passwords and language preferences, is exempt from the e-Privacy Directive, and from the notice and consent obligation.



With the rise of mobile commerce cookies do not work well and they cannot identify the same user across multiple devices. To make up for cookies' shortcomings, advertisers are developing other methods, including authenticated tracking, browser fingerprinting, cross-device tracking, and more. Companies should stay on top of the upcoming revision of the e-Privacy Directive and any relevant regulatory guidance.

THIS CHAPTER COVERED



Neither the GDPR, nor the Data Protection Directive contain any specific rules on the processing of personal data in the retail context. Therefore, 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 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 will 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 and consent, or in some cases legitimate interest, will become key measures for each retailer.

CHAPTER 4

INDIVIDUALS' RIGHTS

In this chapter: New rights for individuals • Redress • Legal claims

4.1. Key individuals' rights concerning their personal data

ARTICLE 15-21 OF THE GDPR

The existing rights of individuals, such as the right to information, correction, or deletion of personal data have been reinforced. New rights have been created, such as the right to be forgotten or right to data portability. With individuals' growing privacy awareness, companies may expect requests aimed at the deletion or limits on the processing of their personal data.

Under the existing **Data Protection Directive**, individuals have basic rights concerning their personal data, including:

- Right to receive certain (minimum) information about the processing of their personal data (right to access).
- Right to object to the processing of personal data if the processing is based on the company's legitimate interests or for direct marketing purposes.
- Right to request correction, deletion or blocking of the processing of personal data if the processing does not comply with the Directive.

Under the **GDPR**, all of the existing rights have been maintained. However, new rights have been created, such as right to be forgotten or right to data portability.

Right to access

Article 15. An individual can ask for confirmation if the company processes his or her personal data and for information concerning:

- The purposes of the processing,
- The categories of personal data processed,
- Data recipients,
- For how long personal data are kept,
- Right to rectification, erasure, restriction of the processing, and objection,
- Right to lodge a complaint with a DPA,
- Source of data,
- Whether his or her personal data are being used for profiling, and
- If data are transferred outside the EEA and what adequate safeguards are being used.

Right to rectification

Article 16. An individual has the right to obtain:

- Rectification of his or her personal data if the data are inaccurate,
- Completion of his or her personal data if the data are incomplete.

Right to erasure (right to be forgotten)

Article 17. An individual has the right to ask for the erasure of his or her personal data where:

- 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 because of his or her particular situation and there are no overriding legitimate grounds for the processing, or the 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 services, such as social networks.

There are limited exemptions from the right to be forgotten (Article 17.3).

Right to restriction of processing

Article 18. An individual has the right to ask for the restriction of the processing of personal data where:

- An individual questions the accuracy of the 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.

Where processing of personal data has been restricted, the data may only be processed with the individual's consent and only for limited purposes.

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. This means that individuals will be able to easily transfer their personal data from one electronic system to another.

An individual has the right to transmit those data to another company without difficulty, where the processing:

- Is based on consent, and
- Is carried out by automated means.

The individual has the right to have the data transmitted directly from one company to another, provided it is technically feasible. This means that companies should make sure that the data is collected in an organised way, so it can be moved.



Further clarification will be needed on what “data provided by an individual” means. For example if consumers register for a loyalty card they provide certain personal data, such as name, address, contact details, family members, etc. Further to that, at each visit to a store when consumers use on loyalty card it captures their buying habits. Based on that, the retailer can create consumer profiles. It is unclear if that data on consumers’ shopping behaviour is data provided by the consumers and therefore covered under the provision. As it stands, this provision could be interpreted requiring a retailer to transfer information on a customer profile into a competing retailer’s system.

The DPAs (Article 29 Working Party) are expected to issue guidance on data portability in the coming months.

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.

An individual may also object to his or her profiling.

If an individual objects, the company may no longer process personal data unless it shows compelling legitimate grounds for doing so and these grounds override the individual's interests, rights and freedoms.

An individual can also object at any time if personal data are processed for direct marketing. In such cases personal data may no longer be processed.

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

An individual can exercise the right to object by automated means using technical specifications (e.g. by browser settings).

Companies' obligations concerning individuals' rights

Companies should have procedures in place to handle requests from individuals within appropriate time. Before the GDPR becomes operational, companies should evaluate whether their IT systems have capabilities to provide information requested by the individuals within prescribed time.

Notification

Companies should inform individuals where they lift a previous restriction of processing of their personal data (Article 18.3).

Companies should communicate any rectification, erasure or restriction of processing to each recipient to whom the data have been disclosed, unless this is impossible or involves disproportionate effort. (Article 19).

When personal data has been made public and an individual has requested the erasure of the data, companies should inform other companies using the data about the erasure request (Article 17.2).

Fees

Companies should respond to access requests free of charge. If an individual asks for any further copies, a reasonable fee may be charged, but only on the basis of administrative costs (Article 15.3).

Other requests (rectification, erasure, rectification, etc.) must be handled free of charge.

Format

If an individual sends his or her request electronically, the company may also provide the information electronically, unless an individual has expressly requested another format, for example on paper.

Timing

Companies must comply with the individuals' requests concerning rectification and erasure without undue delay.

There is no specific time limit prescribed for dealing with requests concerning right to access, restriction of processing, data portability and right to object.

4.2. Redress and legal claims

ARTICLE 77-82 OF THE GDPR

All individuals have the right to effective protection of their rights in court and with the DPAs. This includes the right to compensation for damages. Individuals can exercise these rights in the member state where they live or where the company that has violated their rights is established.

Under the current Data Protection Directive individuals have the right to a judicial remedy for any breach of their rights, and to an administrative remedy before the DPA. Individuals also have the right to compensation for damages suffered. These rights are regulated by the laws of the member states, which means that the exercise of the rights differs across the EEA.

The GDPR has maintained the right to complain to the DPA and the right to file a case in a court, but they have been enhanced. There is a new right to collective redress. As under the current Directive, the exercise of these rights in court will depend on the national judicial system.

Right to complain to a DPA

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

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

Any individual can file a court case against a decision of a DPA or DPA's non-activity if the DPA does not handle a complaint or does not inform the individual within three months on the progress or outcome of the complaint.

An individual may file the case before court of the country where the DPA is established. (Article 78).



A recent example is the decision of the Court of Justice of the EU in the Schrems Case (C-362/14). Max Schrems was not satisfied with the Irish DPA's response to his complaint and he brought the case to the Irish court. The court referred the complaint to the Court of Justice, which invalidated the Safe Harbour Framework and established that each DPA has the right to independently assess the Commission's adequacy decision.

Right to court action

An individual has the right to an effective judicial remedy if he or she thinks that a company has violated their rights.

An Individual shall bring the case before the court of the country where the company is established or where the individual lives. This right is independent of the right to lodge a complaint with a DPA (Article 79).

Right to compensation

An individual who has suffered material or non-material damage resulting from an infringement has the right to receive compensation for the damage suffered.

The company is exempt from liability if it proves that it is not responsible for causing the damage. If more than one company 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).

Right to collective redress

Individuals can ask non-profit organisations whose statutory aims are public interest activities in the data protection field to lodge a complaint on their behalf.

Member states may also allow such organisations to act independently of an individual's mandate (Article 81). This means that they do not need any specific request from an individual.



The right to collective redress is important in the context of security breaches and any data leaks or hacks. A mishandled cyber-attack can have serious financial consequences, but can also affect company's reputation and brand if affected individuals file for collective redress.

OVERVIEW OF THE REDRESS SYSTEM UNDER THE GDPR



DPA

COURT

**Individual may complain
with the DPA**

**Individual may file
a lawsuit**

**Organisation may file
a collective lawsuit**

Where: individuals' place
of residence or work, or where
the violation took place

Where: individuals' place of residence or where the company is established



**Individual may file
a complaint to court
against DPA decision
or DPA's non-activity**

Where: DPA's location

Individual may request
compensation in all
cases of material or
non-material damage

Organisation may
request compensation
for individuals or file a
lawsuit without individu-
al's mandate
if this is provided in
a member states' law



THIS CHAPTER COVERED

Rights

Under the GDPR individuals have the right to:

- Receive certain (minimum) information about the processing of their personal data (right to access);
- Rectification of their personal data if the data is incorrect;
- Erasure of their personal data, if their data is no longer necessary or an individual no longer consents to the processing of his or her personal data (right to be forgotten);
- Data portability;
- Object to the processing of their personal data, in particular for direct marketing purposes; and
- Restrict the processing of personal data.

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. The GDPR has introduced a collective redress for data protection violations.

CHAPTER 5

ACCOUNTABILITY

In this chapter: Key accountability requirements • Data Protection Officer

5.1. Key accountability requirements

ARTICLE 24 AND 30 OF THE GDPR

All companies in all sectors will have to implement compliance programmes to ensure that the way they process personal data complies with the GDPR. Companies will have to demonstrate compliance to DPAs and individuals. One of the significant changes under the GDPR is a removal of the notification duty. This has been replaced by accountability obligation.

Current rules under the **Data Protection Directive** do not explicitly recognise the concept of accountability but companies have certain general obligations, including transparency and data security. Under the Directive, companies are obliged to notify to the DPAs what personal data they collect, for which purposes and with whom they share the data. This obligation was implemented differently across the EEA. In some member states (for example Ireland and the UK), the DPA only needed to receive a high-level summary of data processing activities. In other countries (for example in Austria and France), the DPA requires very detailed explanation of the processing activities. In countries like Germany, there is generally no notification obligation, but companies must appoint a DPO if they employ more than nine people.

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

The accountability principle runs through the core of the GDPR. The GDPR requires that companies implement "appropriate technical and organisational measures" to be able to demonstrate their compliance with the Regulation, which must also include "the implementation of appropriate data protection policies".

Accountability in the GDPR

Accountability means implementing various policies and procedures in order to ensure compliance with the GDPR. Accountability entails establishing a culture of monitoring, reviewing and assessing data processing procedures. It will no longer be sufficient to simply have a privacy policy in place, and review it every other year.


Internal documentation

Companies will have to create and keep internal documentation setting out full details of how they process personal data. (Article 30)

Although the obligation to notify the DPA of data processing has been removed, many companies will have to retain comprehensive records internally. These records will have to be made available to DPAs on demand. In some cases the records will need to be more detailed than notification requirements under the Directive.

The GDPR sets out a detailed list of information that must be recorded. The records should include, for example:


- 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 persons 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, but more clarity is needed on the meaning of the processing which is not occasional.

Policies

Companies will need to put in place comprehensive and clearly drafted privacy policies and privacy notices for individuals. These have to include full details of the processing of personal data, including the legal basis of the processing, the safeguards in place for international transfers and data retention periods. (Article 24).

Companies will also need to establish additional documentation describing rights available to individuals and how these rights can be exercised.

 Under the current rules some websites copied and pasted privacy notices and policies from other sources they could easily find online, but without much thought. This approach will be much more risky under the GDPR. To produce a valid policy, companies will have to have a thorough knowledge of how they use personal data.

Privacy by design and by default

The Regulation 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 20). 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

This concept means that a privacy compliant approach is embedded in technologies, products and services in the whole cycle of data processing.

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 privacy by design principles which have not been included in the GDPR, but are broadly recognised standards.

Following these principles might help companies implement practical steps to achieve privacy by design.

1. Use proactive rather than reactive measures; anticipate and prevent privacy-invasive events before they happen.
2. Personal data must be automatically protected in any IT system or business practice.
3. Privacy must be embedded into the design and architecture of IT systems and business practices.
4. All legitimate interests and objectives are accommodated in a positive-sum manner.
5. Security is applied throughout the entire lifecycle of the data involved.
6. 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.
7. 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

This concept means that companies should implement measures for ensuring that, by default, they only process personal data which are necessary for each specific purpose.

This obligation applies to:

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

Privacy Impact Assessment (PIA)

Under the current **Directive**, there is no requirement to assess the impact of data processing.

Under the **GDPR**, such an assessment will be required if the planned data processing is likely to result in high risks to individuals, including where processing involves "new technologies" or "large scale processing". (Article 35)

Requirements and procedure for a PIA

Under the GDPR a PIA is required in the following cases:

- 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.

A PIA must be carried out before the risky processing begins. A PIA should include:

- A description of the processing operations and their purposes, including the company's legitimate interest;
- An assessment of the necessity and proportionality of the processing operations in relation to these purposes;
- An assessment of the risks to the rights and freedoms of individuals;
- The measures to address the risks, including data security measures.

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

Where necessary, in particular when the risks have changed, companies should assess whether the processing complies with the PIA and whether any PIA review is necessary.

Consultation

Anytime a PIA is required, companies should consult the DPO.

Where appropriate, companies should seek the views of individuals concerned or their representatives. The timing and format of the consultation required is unclear. It is also unclear what the effect of any objection would be. However, there is a vague safeguard that the company's commercial interests or the security of processing should be taken into consideration.

PIA standards

The DPAs are expected to publish a list of the types of processing operations which require PIA and may also publish a list of those which do not require PIA.

DPA consultation

Under the **GDPR** it is no longer necessary to notify the DPA about the processing activities. However, some notification requirements remain (Article 36).

If the PIA 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 after receiving the request for consultation to provide written advice to the company. This period may be extended by 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.

Adherence to codes of conduct

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

Pseudonymous data

The GDPR introduces a new concept of data pseudonymisation. Pseudonymous data is still personal data and therefore, not exempt from the GDPR. However, companies that render data pseudonymous face lighter compliance regimes in some areas.

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. This process may create useful datasets, for example aggregated data on consumer preferences and shopping habits, while limiting privacy risks.

The GDPR includes incentives to pseudonymise personal data.

- It will be easier for companies that pseudonymise personal data to process personal data for secondary purposes beyond the original collection purposes (Article 6.4.e).
- Pseudonymisation makes compliance with the security requirements easier. 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 would still need 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.

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.

Data Protection Officer (DPO)

For more information see the next section on the DPO.

5.2. Data Protection Officer (DPO)

ARTICLES 35-37 OF THE GDPR

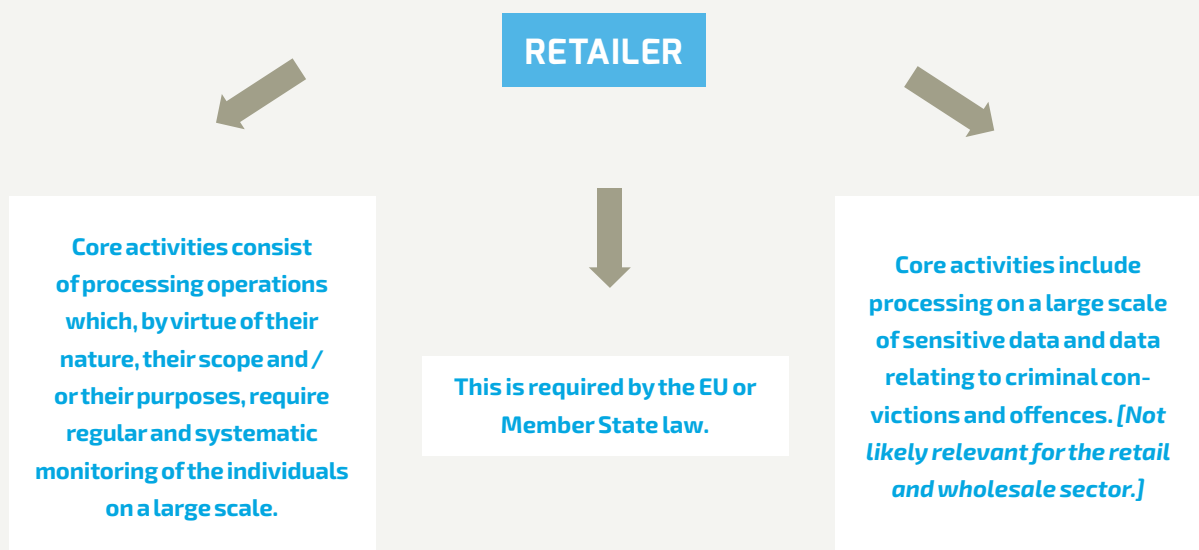
All companies that process personal data in certain circumstances (when their core activities involve systematic monitoring of individuals on a large scale) must appoint a data protection officer ("DPO"). The DPO is responsible for monitoring compliance with the GDPR and for reporting to the management on privacy-related issues.

Under the current **Data Protection Directive**, there is no mandatory requirement to appoint a DPO. The Directive leaves it up to the member states to regulate the DPO appointment and tasks. Member states may also exempt companies that have appointed a DPO from the duty to notify the processing to the DPA. Requirements differ across the EEA.

In some countries the DPO is mandatory and this function is expressly regulated (Germany). In other countries the DPO is optional but there are certain advantages of appointing one (France, Luxemburg, the Netherlands, Norway, Sweden). In many countries there are no specific rules (Austria, Czech Republic, Ireland, and the UK).

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.

WHEN COMPANIES NEED TO APPOINT A DPO



It is unclear what core activities and large scale mean. It seems to cover companies who deal with big data. Monitoring in the GDPR generally means online behaviour tracking or profiling activities. **This could mean that only companies that track and profile on a large scale and this is core to the business have to appoint a DPO. Many brick & mortar shops and 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.**


*The DPO requirements are unclear.
Companies should stay up to date with any regulatory guidance.
The DPAs (Article 29 Working Party) are expected to issue guidance on the DPO in the coming months.*

DPO appointment and tasks

Expert knowledge

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 good knowledge of the GDPR and the relevant local applicable laws, good knowledge of the company and its business, and at least basic knowledge of IT and security issues.*


Internal or external expert

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

- If a DPO is an employee, the appointment should be explicitly 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 explicitly documented in a written service contract. The DPO can be either a natural person or a legal entity (for example a consultancy or a law firm).

Location

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

 *It is unclear what "easily accessible" means. This is likely to mean that the DPO must at least be resident in the EEA. Although the location of a DPO is not strictly specified, it may nonetheless be practical for some companies to appoint country specific DPOs. This is because the DPO should be familiar with the processing taking place in a particular country and may be required to communicate with the local DPA in the event of questions.*

Length of the appointment


The length is not specified in the GDPR. This means that the DPO can 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:

- **To inform and advise the company and the employees who are processing personal data of their legal obligations.**

 *In practice this means identifying ongoing data protection operations and providing advice to the management and relevant personnel relating to the processing of personal data, such as:*

- *Liaising with HR in relation to the development of policies, procedures and practices and for staff member of staff and job applicants,*
- *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, advertising, profiling and publicity,*
- *Ensuring that policies concerning access and correction rights are in place,*
- *Ensuring that personnel with access to personal data have received appropriate training,*
- *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 internal 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. The DPO may not need to respond directly, but must be able to refer the request to the appropriate person (e.g. customer service or HR). The DPO may adopt, or assist in adopting, procedures for handling privacy complaints.

- **To provide advice, where requested, as regards 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, companies may need to take some or all of the the following measures:

- Ensure that the DPO is properly and in a timely manner involved in all data protection issues.
- 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.
- Allocate budget for carrying out privacy projects effectively. The DPO should have the necessary resources and time to attend professional trainings, be a member of professional associations, and keep up to date with data protection developments and relevant DPA guidance.
- 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.
- Ensure the DPO is appropriately remunerated so that this does not affect his or her autonomy or independence.
- Ensure that the DPO has sufficient access to information about the company's data processing.
- Provide for secrecy or confidentiality clauses concerning the performance of the DPO's tasks.
- 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 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 in certain circumstances must 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. The requirement to appoint a DPO will require clarification from the DPAs but it is likely to apply to companies that track and profile individuals on a large scale and this is core to their business. Many brick & 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.

CHAPTER 6

DATA SECURITY

In this chapter: General security obligations • Data breaches • Cybersecurity

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 financial 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 is 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 the recent years, retailers have become one of the most targeted industries when it comes to security threats. Therefore, the theft of consumer data has become as important concern for retailers as merchandise theft.

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.

The current **Data Protection Directive** includes general rules requiring companies to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks involved in the processing of personal data. There are no specific rules prescribed at EEA level. Many member states have adopted specific rules on IT and physical security, data retention and disposal policies, security policies and security audits, passwords, data security breaches, etc.

Data security plays a prominent role in the **General Data Protection Regulation**. Under the GDPR, similarly to the Directive, companies 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. Unlike the Directive, however, the GDPR provides specific suggestions for what kinds of security actions might be considered appropriate to the risk. These risks are, for example: 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

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 bricks & mortar shop or a small online shop (with a relatively small number of customers and employees) are likely to have different security risks and different obligations compared to a global omni-channel retailer with operations in many countries.

Basic security requirements

The GDPR mentions the following basic security measures, without, however, providing any further 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.

For additional guidance on security standards, controllers and processors may consider the Recitals of the GDPR, in particular Recitals 49 and 71, which allow for processing of personal data in ways that may otherwise be improper when necessary to ensure network security and reliability.

Codes of conduct

Adherence to approved codes of conduct or approved certification mechanisms may be used to demonstrate compliance with the security requirements.

Breach notification

Personal data breaches must be notified to the DPAs, and in certain situations to individuals. (for more details see the next section)

Use of service providers

Compared to the Directive there are detailed requirements regarding the use of the service providers. Service contracts will have to oblige processors to assist controllers to comply with certain obligations, including general security, breach notification, and data protection impact assessment.

Service providers who handle personal data, are directly responsible for various matters, including security.

Existing outsourcing contracts will need to be tracked, considered and renegotiated to reflect the tighter security requirements.

Other matters

Companies will have to implement appropriate measures in order to ensure that the personal data processing meets GDPR requirements, including "security by design and default". This would affect the design and delivery of new products or services as well as the existing ones.



For example, as retailers increasingly roll out mobile solutions, security for devices, applications and content should be an important concern in any mobility management strategy.

Suggested strategies for basic security measures

Companies should make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff. Here are some basic security tips that companies might implement.

Make a data inventory

Take stock of personal data (for example, customer files, contracts, employee data) and the processing that relates to the data, whether the processing is automated or not, and how the processing is carried out.

Identify the risks

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.

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.

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.

Encryption. Ensure, for example via encryption, 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 on the system.

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.

Business continuity and crisis response. Implement appropriate disaster recovery plans. Ensure that personal data is protected against accidental destruction or loss by taking encrypted backups and hosting personal data in a secure manner. Have clear procedures setting out who is responsible for consumer and media questions following a breach.

Audit. Audit security systems whenever necessary.

6.2. Personal data breaches

ARTICLE 33-34 OF THE GDPR

The use of digital technology means that 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. When it comes to security breaches, consumers believe that retailers have the primary responsibility for keeping their information safe. Retailers need to take security seriously or risk losing customers. Protecting data by minimum security is no longer sufficient.

What is considered a data breach

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.

The current **Data Protection Directive** does not have any specific provisions about data breaches. Approaches vary across the EEA. Some member states require companies to notify breaches (e.g., Austria, Germany, Norway, Spain). In some other countries reporting is voluntary (e.g., Belgium, Denmark, Ireland and the United Kingdom). In most other countries there are no specific rules or guidance.

The **GDPR** introduces a general obligation to report data breaches for all companies in all sectors, irrespective of their size and the risks involved in the data processing.

Businesses in all sectors must notify the breach to:

a. Competent DPA

Any breach without undue delay and where feasible not later than 72 hours after having become aware of the breach – unless the breach is not likely to result in a high risk to the rights and freedoms of individuals.

b. Affected individuals

Any breach that is likely to result in a high risk to the rights and freedoms of individuals – without undue delay.

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).



	<p>NEW OBLIGATIONS CONCERNING DATA BREACHES IN DETAIL</p>
<p><i>General reporting obligations</i></p>	<p>Companies have a general obligation to report data breaches to:</p> <ul style="list-style-type: none"> • Competent DPA – any relevant breach without undue delay and where feasible not later than 72 hours after having become aware about the breach. • Affected individuals – any relevant breach without undue delay.
<p><i>Breaches that must be notified</i></p>	<p>Any breach that is likely to result in a high risk to the rights and freedoms of individuals.</p> <p>Risks may result in physical, material or moral damage to individuals such as 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. (Recital 75)</p>
<p><i>Reporting breaches to the DPA</i></p>	<p>When Without undue delay and where feasible no later than 72 hours after discovering the breach. If it is not possible to notify the DPA within 72 hours, this delay must be justified.</p> <p>What The report should describe:</p> <ul style="list-style-type: none"> • The nature of the breach including where possible, the categories and approximate number of individuals affected and the categories and approximate number of data records concerned; • Name and contact details of the DPO or other contact point where more information can be obtained; • The likely consequences of the breach; • Measures taken or intend to address the breach, and measures to mitigate its possible adverse effects. <p>Exemptions None.</p>
<p><i>Reporting breaches to affected individuals</i></p>	<p>When Without undue delay</p> <p>What Inform the individuals about:</p> <ul style="list-style-type: none"> • Name and contact details of the DPO or other contact point where more information can be obtained; • The likely consequences of the breach; • Measures taken or intend to address the breach, including to mitigate its possible adverse effects. <p>Exemptions Affected individuals do not need to be informed if:</p> <ul style="list-style-type: none"> • A company has implemented appropriate security measures, and applied them to the data affected by the breach. For example, the data was encrypted or rendered unintelligible to any person who is not authorised to access it; • A company has taken subsequent measures ensuring that the high risk for the rights and freedoms of individuals is no longer imminent; • It would involve disproportionate effort (for example thousands of people were affected). In such case, companies should issue a public communication or similar measure informing individuals in an equally effective manner.
<p><i>Other obligations</i></p>	<p>Any data breach must be documented, including facts surrounding the breach, its effects and the remedial action taken. The documentation should be available to the competent DPA.</p>

Suggested strategies for data breaches

Before the GDPR takes full effect, companies should prepare for how they will prevent and react to data breaches once they occur. Companies should assess the overall state of security to ensure that data breaches can be promptly detected and managed.

a. Companies should consider these measures to prevent data breaches, and prepare a plan to follow in the event of a breach (Breach Response Plan).

Develop and implement a data breach response plan, including for example 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, 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.

Inform employees about when, how and to whom they must report a data breach. Ensure that third party service providers are properly informed about the incident plan and procedures, and in particular of their responsibility to notify the company about any breach that occurs on their side.

Consider encrypting the data or implementing other measures that will make the data unintelligible. This may exempt a company from notifying the affected individuals and may help prevent harm to the business reputation.

Ensure that agreements and contracts with third party service providers (data processors) include appropriate security measures.

b. Once a breach has occurred companies should consider these steps to deal with its consequences.

Gather as much information as possible, including types of compromised data, in particular if data was sensitive.

Assess the breach, its scale, the individuals that may be affected and the possible consequences. Prepare a report describing the breach and its scope.

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.

Establish which is the relevant DPA that needs to be notified. Where individuals must be notified, establish how many of them are affected, what data types are involved and whether the breach will have a harmful effect.

Determine content and format of information notice. Ensure that any notice about the breach complies with legal requirements.

Notify competent DPA about any relevant data breach without undue delay and where feasible not later than 72 hours after having become aware about the breach. Notify affected individuals about any relevant breach without undue delay.

Consider engaging an external service provider to deal with notifications to individuals.

When notifying individuals, personalised e-mails or telephone calls may be necessary, but where a significant number of individuals are affected, a communication in the press may be sufficient.

Consider engaging a PR agency to analyse media coverage, manage responses, and minimise potential damage to the company's reputation.

c. Companies should document the breach, including relevant facts, the effect of the breach, and the remedial action taken to prevent recurrence.

6.3. Cybersecurity

NETWORK AND INFORMATION SECURITY DIRECTIVE

In parallel with the GDPR, the EU has adopted a Directive on security of network and information systems. This establishes a common level of network and information security (NIS) throughout the EU. Currently there are varying and fragmented approaches across the EU. The Directive sets out EU-wide cybersecurity obligations for operators of essential services and digital service providers, including online platforms.

Which companies are covered by the Directive?

The Directive of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (EU) 2016/1148 - the Network and Information Security (NIS) Directive - imposes obligations on operators in **essential service sectors and digital service providers** to take appropriate security measures designed to manage cyber risks and to report major security incidents.

- **Digital service providers** include **online marketplaces**, online search engines, and cloud computing services.
- **Essential service sectors** include energy, transport, banking, financial market, health, water supply & distribution and digital infrastructure.

What does the Directive mean for digital service providers and retailers?

Companies that manage online marketplaces will be affected by the NIS Directive and will have additional security and reporting obligations. The Directive requires them to take appropriate security measures and report incidents to the appropriate authorities. Micro and small enterprises are exempt from these requirements.

The Directive expressly requires digital service providers to establish appropriate and proportionate security measures.

Digital service providers will be required to report any incident that has substantial impact on the services they provide. This could take into account, in particular, the number of users affected by the incident, the duration of the incident, its geographical spread, the extent of the disruption to the functioning of the service.

In addition to the general data breach notification requirement in the GDPR (see section 6.2), under the NIS Directive digital service providers will have to notify incidents without regard to whether personal data was impacted, instead focusing on whether the incident had a "substantial impact" on the service.

Where companies fail to comply with the security and incident-reporting obligations, enforcing authorities will take action. The Directive leaves open the question of what penalties will exist for non-compliance with these requirements.

After the NIS Directive has entered into force, the Commission will have 12 months to adopt implementing acts. This work will be developed by the European Agency for Network and Information Security (ENISA). Member states will have 21 months to adopt the necessary national provisions.



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 OUTSOURCING AND OFFSHORING

In this chapter: Service providers • Data transfers outside the EU

7.1. Engaging service providers

ARTICLE 28 OF THE GDPR

Using service providers to process personal data requires an appropriate contract committing the service provider to comply with data protection rules. 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

Under the current **Data Protection Directive**, there are no specific rules on contractual arrangements with service providers and service providers' liability. However, service providers must ensure data security. Some member states lay down specific rules on what must be included in a service contract (for example Germany).

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/vendors (data processors) and companies that engage them because it imposes direct compliance obligations and sanctions on service providers. The Regulation imposes detailed obligations and restrictions directly on processors, unlike the current Directive that only applies to data controllers. There are significant penalties for processors who fail to comply with their new responsibilities.

The new law is prescriptive about the detailed contract requirements that will need to be in place when a service provider is engaged, whether external or internal (e.g. affiliates in the same group).

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.

New obligations for outsourcing

Contract terms

Companies engaging a service provider must ensure 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 service provider.

The service providers must comply with the following requirements:

- 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 service provider intends to use a subcontractor, companies must agree to this in writing (either via a general authorisation or specific contractual terms).

In case of a general authorisation, the service provider must inform the company of any intended addition or replacement of other processors, so the company may object such changes.

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

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

Codes of conduct and certification

Companies may only appoint service providers that provide sufficient guarantees they can comply with the GDPR obligations.

If the service provider is signatory 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.

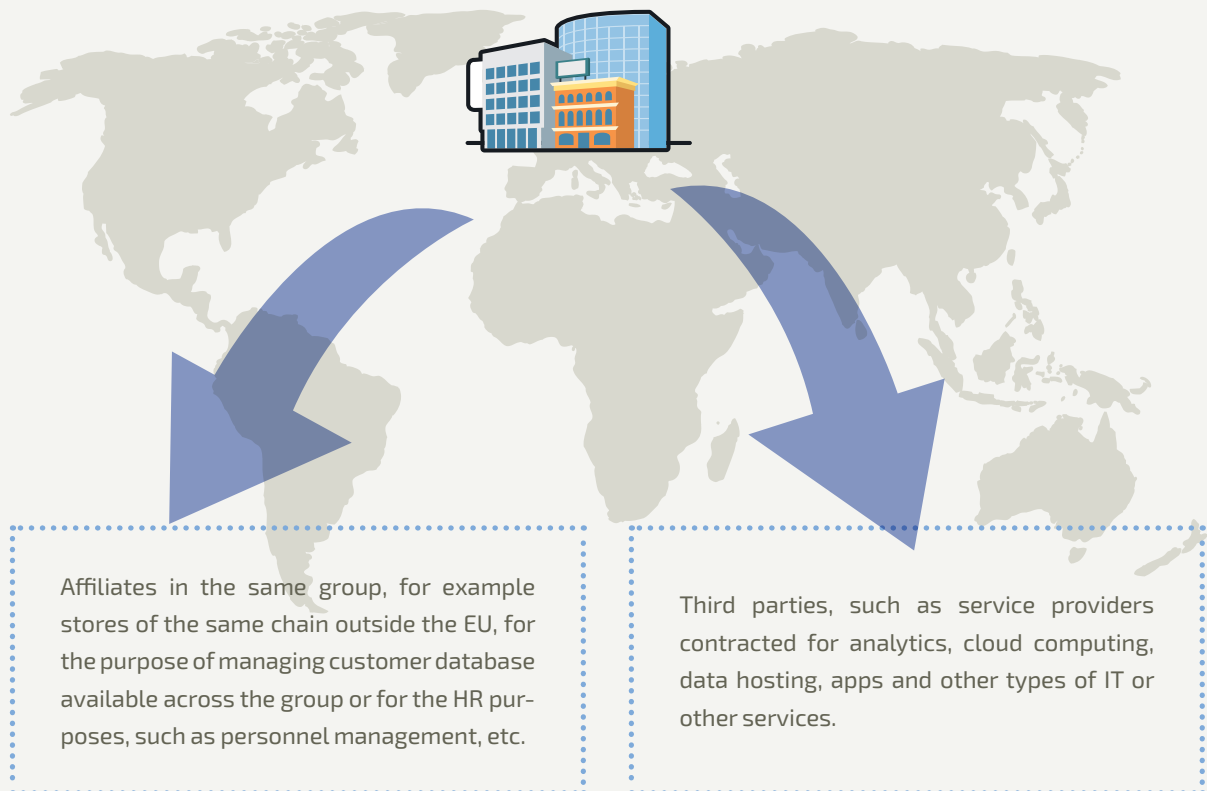
7.2. Basic principles on transferring personal data outside the EEA.

ARTICLE 41-44 OF THE GDPR

Increasing numbers of companies are moving their IT systems offshore, including to low-cost countries. Personal data can flow freely between companies and individuals in the EEA. However, there are restrictions for transferring personal data outside the EEA.

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 EEA, but can be viewed, accessed, copied, etc. by anyone outside of the EEA, this is considered to be data transfer.

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



The current **Data Protection Directive** restricts the sharing of personal data with countries outside the EEA. Transfers of personal data from the EEA to non-EEA countries are prohibited unless the third country to which personal data are transferred ensures an adequate level of protection. If the transfer is to a non-EEA country without adequate safeguards (e.g., to the U.S.), companies in the EEA must put in place adequate safeguards.

The restrictions on data transfers from companies transferring personal data from the EEA to companies receiving personal data outside the EEA will continue under the **GDPR**. Many rules will remain similar, but some new rules have been added. For example, the binding corporate rules (BCRs, explained below) have been formally recognised and procedures for their approval have been simplified. There are more transfer options, such as standard and ad hoc standard clauses and codes of conduct adopted or authorised by the DPAs. No specific DPA authorisation for transfers based on Standard Contractual Clauses will be required. Companies relying on these Clauses will face significantly reduced administrative burden and simpler transfer procedure.

When can companies transfer personal data outside the EEA?

1. The third country ensures an adequate level of protection

Under the GDPR, as under the current Directive, transfers to countries that ensure an adequate level of protection are regarded as if they were transfers within the EEA. Such transfers do not require any specific authorisation from the DPA.

The European Commission decides which countries ensure adequate level of protection (adequacy decision). The Commission's decisions adopted under the 1995 Directive will continue to be valid under the GDPR until replaced or repealed.

The following territories have been so far deemed adequate by the Commission: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the EU-U.S. Privacy Shield (more information on the Privacy Shield in the next section)

The Commission's decisions shall be reviewed at least every four years (for the EU-U.S. Privacy Shield, annually). The Commission may decide to repeal, amend or suspend the decisions.



According to the Court of Justice of the EEA (CJEU) judgement in the Schrems Case (c-362/14) any DPA may challenge the Commission's adequacy decision. This means that any DPA can suspend the transfer of personal data to the country found adequate. In the Schrems Case, the CJEU found the Safe Harbour framework, which was used to facilitate data transfers to the U.S., to be invalid because it did not ensure an equivalent level of data protection. This was because U.S. law did not provide adequate limitations on government surveillance, Europeans did not have access to effective legal remedies and no judicial redress in the U.S.; and Safe Harbour was not binding on the U.S. public authorities and allowed governmental access to personal data. (See Privacy Shield below)

2. A company has put in place adequate safeguards

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

2.1. BCRs

The Binding Corporate Rules (BCRs). BCRs are data protection policies adopted by a company in the EEA for data transfers outside the EEA within a group of companies engaged in a joint economic activity. BCRs must be approved by the DPAs. BCRs have existed before, but the GDPR now officially recognises them (more information on BCRs in the next section).

2.2. Contract

There is a contract between the EEA company and the recipient located outside the EEA and the contract is based on the Standard Contractual Clauses ("Clauses"). The Clauses are a contract template adopted by the Commission or by the DPA and approved by the Commission. Companies may not deviate from this standard contract template (more information on the Standard Contractual Clauses in the next section).

There is an ad-hoc contract between the EEA company and the recipient located outside the EEA and the contract is not based on the Standard Contractual Clauses. Such contracts must be approved by a DPA.

2. 3. Consent

The individual has consented to the transfer of his or her personal data. Consent may be used for specific single transfers, but not for routine mass data flows. Obtaining consent is often difficult and impractical, especially for transferring employee data (more information on consent in the next section).

2. 4. Code of conduct or certification

An approved code of conduct or an approved certification mechanism together with the binding and enforceable commitment of the company in the third country to apply the appropriate safeguards. This transfer mechanism is new under the GDPR.

2. 5. Exemptions

Other specific conditions ("derogations") apply, such as: transfer is necessary for contractual purposes, for important public interest reasons, for establishing, exercise or defence of legal claims, to protect individuals' vital interests, or transfer is made from a public register. These criteria are interpreted very narrowly.

If the company cannot rely on the contract or BCRs and no other derogation is available, 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.

How to decide which data transfer mechanism to use?

In order to determine which data transfer mechanism is most suitable, a company will need to identify and analyse what personal data are being processed, what data will be transferred and for which purposes, including:

- Types of data being transferred;
- Types of individuals whose data are being transferred;
- Purpose(s) of the transfer;
- Systems or applications used for the data transfer;
- Senders and recipients of the data (company departments);
- Third parties who have access to the data or to whom the data are disclosed);
- Security measures implemented by the data recipients;
- Key data flows carried out in the context of the company's core operations:
 - From which EEA countries the transfers take place.
 - The type of data (e.g., employee data, customer data).
 - How sensitive the data is (e.g., health information, trade union membership),
 - How important the data is to the company's business;
 - Where would the company most likely face a complaint (works council, a DPA).

7.3. Selected data transfer mechanisms

ARTICLE 41-44 OF THE GDPR

Binding Corporate Rules (BCRs)

BCRs are a set of internal rules that allow multinational companies to transfer personal data from the EEA to their affiliated companies located outside the EEA. BCRs ensure that a single set of rules apply throughout the group instead of various contracts.

BCRs are often seen as a global privacy policy based on EEA principles, rather than just a data transfer instrument. 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.

BCRs must be internally binding within the corporate group, the parent and its subsidiaries. All employees must be bound to comply with the BCRs.

The concept of the BCRs was developed by the DPAs (the "Article 29 Working Party"). The practice concerning the establishment and approval of BCRs differs across the EEA. The GDPR sets out harmonised rules and approval procedure. In order to become effective, BCRs must be approved by the DPAs in all countries from which personal data are transferred. In order to streamline the process, the GDPR has developed some cooperation methods among the DPAs, for example, a mutual recognition system.

BCRs are based on the accountability model, as they promote high internal privacy standards. Companies that wish to prepare for the accountability obligations under the Regulation can put themselves in a good position if they decide to implement BCRs. However, establishing BCR's compliance and putting a document in place, requires significant resources.

Standard Contractual Clauses

Data transfer agreements can be either ad hoc (i.e. individually negotiated by the companies and approved by the DPAs) or can incorporate Standard Contractual Clauses (SCC).

The SCC include a set of unamendable contractual terms concerning rights and obligations of the parties as well as liability for violations and an annex with a description of the transfer including categories of personal data transferred, data recipients and purposes of the transfer. The information in the annex is provided by the companies. Each legal entity transferring and receiving personal data must individually sign the SCC.

There are two different types of SCC:

- Clauses for transfers to **data controllers (C2C Clauses)** used for transfers from the EEA companies to non-EEA companies, which are authorised to make independent decisions about the personal data received (data controllers).
- Clauses for transfers to **data processors (C2P Clauses)** used for transfers to service providers located outside the EEA.

There are advantages on relying on the SCC. For example, they consist of legal terms that are the same and consistent across the EEA.

However, the SCC are static documents that cover a concrete set of personal data and purposes for which the transfers are taking place. Therefore, the information about transfer provided in the annex must be reviewed and amended as changes occur in data flows. For more complex data flows, keeping track of the changes may become very burdensome.

Each party to the Clauses is liable to the other parties for damages caused by a breach of the Clauses.

Privacy Shield

Privacy Shield is the new, improved Safe Harbour, which it replaces. The Safe Harbour agreement was declared invalid by the EU Court of Justice in October 2015 in the Schrems Case. It guarantees that privacy protections for data transferred to the U.S. are equivalent to data protection standards in the EU. There is a stronger enforcement for authorities in the EU and the U.S., and more robust protections against access to personal data by the U.S. security agencies.

Under the Privacy Shield, as under Safe Harbour, U.S. companies that receive personal data from the EEA will have to comply with the privacy principles: notice, choice, security, data integrity and purpose limitation, access, accountability, and recourse, enforcement and liability. Companies will self-certify that they meet the requirements and will register to be on the Privacy Shield List. Companies will have to recertify annually.

Compared to Safe Harbour, there are tighter conditions for onward transfers (when the receiving company subcontracts to third parties).

Monitoring and oversight from the Department of Commerce will be stronger and more proactive than under Safe Harbour. This will include assessment of whether companies' privacy policies are in line with the Privacy Shield principles. These reviews will take place in case of specific complaints, when a company does not provide satisfactory responses, or when there is evidence suggesting that a company does not comply with the principles.

In case of non-compliance, U.S. companies will risk sanctions and removal from the Privacy Shield list.

Any individual whose personal data has been misused will have various possibilities for redress, including lodging a complaint with the company, lodging a complaint with the competent DPA (who will refer the complaint to the Department of Commerce), using the alternative dispute resolution (ADR), which will be free of charge.

Companies have been able to sign up to the data transfer agreement from August 1. According to the U.S. Department of Commerce, Microsoft and Salesforce are among the biggest of the 34 companies to have self-certified. More information is available on the Privacy Shield website <https://www.privacyshield.gov>.

Consent

Another option is to obtain the individual's consent. However, in practice, transfers based on consent are narrowly permitted by the DPAs and therefore, not very practicable. According to the guidance from the Article 29 Working Party, transfers should rely on consent only "where it would be genuinely inappropriate, maybe even impossible" for the transfer to take place using other adequate safeguards.

There are some advantages of consent, for example it works for transfers that must take place at short notice, this is a quick and flexible tool. However, generally consent is impracticable.

- Consent must be explicit, free, specific and informed.
- Consent must be specific, which means that blanket or generic consent is not valid. The individual must give consent to a particular transfer or a particular category of transfers.
- Consent is insufficient for future transfers, when the occurrence and recipients are not known.
- Consent is not an adequate long-term framework for regular transfers, such as centralisation of global employee or customer databases.



THIS CHAPTER COVERED

Engaging service providers

The Regulation imposes detailed obligations and restrictions directly on processors, unlike the current Directive that only applies to data controllers. There are significant penalties for processors who fail to comply with their new responsibilities. The new law is prescriptive about the detailed contracts that will 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: New enforcement powers • One-Stop-Shop • Sanctions for violations

8.1. Data Protection Authorities (DPAs) and One-Stop-Shop

ARTICLE 51-79 OF THE GDPR

Data protection authorities will have increased enforcement powers, including imposing substantial fines. 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 are covered.

Currently, under the **Data Protection Directive**, each member state has its own independent public authority responsible for monitoring and enforcing compliance with the data protection law. These authorities have local investigative and enforcement powers. There is no cooperation mechanism for cross-border violations. If companies are established in more than one member state, they fall under the jurisdiction of the DPA in each of these states. Often, the DPAs enforce diverse data protection requirements, produce different guidance and set different enforcement priorities. Companies that operate in the plethora of various obligations and enforcement standards face additional compliance costs and risks.

In order to ensure more coherence in its application, the **GDPR** creates a One-Stop-Shop supervisory and cooperation mechanism among data protection authorities. This means that companies that operate in many member states are subject to the authority of one "lead" DPA, supervising all cross-border processing activities of this company.

The "lead" DPA is the DPA of a company's single or main establishment (i.e. the place of its central administration) of a company. This "lead" DPA must closely involve and cooperate with other concerned DPAs in reaching its decisions.

GDPR includes rules to identify which DPA takes the lead when it comes to privacy violations with an international dimension, for example where individuals in many member states have been affected.

In a traditional headquarters/branches organisation, the lead DPA is usually quite easy to determine. This is more difficult for complex, multi-site companies, where decisions about specific processing activities may be taken in a number of different places.

In case of uncertainty, companies should map out where the company makes its most significant decisions about data processing. This will help to determine its "main establishment" and thus the lead DPA.

Other "concerned" DPAs remain competent to investigate and enforce data protection law 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 it - 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 a period of 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 it does not wish to intervene, the DPA will carry out the investigation on its own.

8.2. Sanctions

ARTICLE 83-84 OF THE GDPR

Any company can have sanctions imposed on it for any violation of any provision of the GDPR. Compared to the existing rules, the likelihood of enforcement and subsequent sanctions are significantly higher.

Under the current **Data Protection Directive**, sanctions vary significantly across the EEA. For example, the current maximum fine in the UK is £500,000, in Germany and France EUR 300,000, in Spain EUR 600,000, and in Portugal up to EUR 30,000. In some countries, possible sanctions also include imprisonment. Sanctions can only be imposed on data controllers.

Under the **GDPR** sanctions will apply not only to data controllers, but also to data processors that have breached their obligations. The Regulation sets out the same sanctions across the EEA and significantly raises their level. It also harmonises the approach to enforcement across the EEA.

In case of violations of the Regulation, the competent DPA can impose certain regulatory measures, such as issuing warnings or reprimands, imposing temporary or definitive limitations, including a ban on data processing. The DPAs can also issue fines.

There is a significant increase in the potential severity of sanctions. Each DPA can impose fines, in addition to or instead of corrective measures. This shall depend on the circumstances of each individual case.

The DPAs enforcement powers

Under the GDPR the DPAs will have the following **investigative powers**:

- Order a data controller and the processor (or applicable representative) to provide any information it 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 and processor including data processing equipment.

Under the GDPR the DPAs will have the following **corrective powers**:

- Issue warnings to a data controller or processor that intended processing is likely to result in infringement of the GDPR;
- Issue reprimands to a data controller or processor where processing operations have infringed provisions of the GDPR;
- Order a data controller or processor to bring processing operations into compliance with the GDPR (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.

Factors for the DPAs to consider when imposing a fine

- The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of individuals affected and the level of damage;
- The intentional or negligent character of the infringement;
- Any action taken to mitigate the damage suffered by the individuals;
- The degree of responsibility of the company taking into account implemented security measures, and data by default and by design measures;
- Any relevant previous infringements;
- The level of cooperation with the DPA in order to remedy the infringement and mitigate its adverse effects;
- The categories of personal data affected by the infringement;
- The manner in which the infringement became known to the DPA, in particular whether, and if so to what extent, the infringement has been notified;
- Where enforcement measures have been already imposed and the same violation took place;
- Adherence to approved codes of conduct or approved certification mechanisms;
- Any other aggravating or mitigating factor, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Overview of the fines

According to the GDPR, fines imposed by DPAs should be effective, proportionate and dissuasive. However, if a company responsible for the same or linked processing operations intentionally or negligently, infringes several provisions, the maximum fine that can be imposed cannot exceed the fine for the gravest single infringement.

In such cases companies will be liable to:

a. Fines up to 10 000 000 EUR or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, for the violation of the provisions concerning for example:

- A child's consent;
- Processing not requiring identification.
- Obligations for the controller for the joint controllers, for representatives of controllers not established in the Union, for the processor, for the person processing under the authority of the controller and processor;
- Obligation to:
 - Maintain a record of processing activities
 - Co-operate with the DPA
 - Ensure appropriate security
 - Notify data breach;
- Data protection impact assessment and the DPA prior consultation;
- Appointing a DPO;
- The obligations imposed by the certification body.

b. Fines up to 20 000 000 EUR or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher for the violation of the provisions concerning for example:

- Basic principles related to personal data processing, lawfulness of processing, to conditions for consent and to the processing of special categories of personal data.
- Individuals' rights: information on the exercise of the rights, rights in relation to recipients, right of access the data, right to rectification, right to erasure, right to restriction of processing, notification obligation, right to data portability, right to object, right not to be subject to automated individual decision making, including profiling.
- Transfers of personal data outside the EEA to recipients not deemed to provide adequate protection.
- Any obligation for specific data processing situations, in particular, for journalistic purposes, employment context, public interest.
- Non-compliance with an order or a temporary or definite limitation on processing, or the suspension of data flows by the DPA as to comply with the individuals' requests, to communicate a personal data breach to the individual or does not provide access to information necessary to its tasks.
- Non-compliance with a DPA order.



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 to 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 than under the current legislation, and enforcement will be more coordinated across the EU.

CHAPTER 9

PRIVACY IN THE WORKPLACE AND OTHER ISSUES REGULATED NATIONALLY

9.1. Privacy in the workplace

ARTICLE 88 OF THE GDPR

The GDPR does not harmonise the rules on the processing of personal data in the employment context. This is because the processing of personal data of employees is closely related to employment law, which differs across the EEA. Member states may adopt specific rules on privacy in the workplace, covering processing of personal data for the purpose of recruitment, the 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.

Retailers and employee personal data

Any retailer employing staff processes HR data on a daily basis.

The **Data Protection Directive** does not deal with any specific aspect of an employment relationship. In particular, it does not provide any specific rules on what categories of personal data employers may collect from the employees, for which purposes they may use the data, how long they may retain the data, what rules the employers should follow if they monitor the employees. The Data Protection Directive only sets out general provisions on the collection and processing of personal data. These provisions are then further interpreted by individual member states, which implement them in their national legislation. This means that in each EEA member state, there are different rules on employee privacy.

Under the **General Data Protection Regulation**, member state law will continue to differ in the context of HR data processing and employment law. Member state law or collective agreements may provide for specific rules on the processing of employees' personal data.

In particular, these can cover conditions under which personal data in the employment context may be processed, based on the consent of the employee. These can also cover the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work. They can further cover the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and the termination of the employment relationship.

Things to remember when dealing with employee privacy

Member states may adopt their own data protection laws covering the processing of personal data in the employment context. This will likely lead to further fragmentation in this area.

Companies should stay up to date with the existing applicable laws in the country where they have employees. **Companies should closely monitor if these member states implement specific employee data protection rules.**

Companies should audit how HR data are being processed and what steps are necessary to ensure compliance with the GDPR. HR and data protection functions should be aligned in order to ensure compliance with the new requirements

When will it be legal to process employee personal data?

Many companies currently process employees' personal data on the basis of their consent. This has been criticised in the past. Many DPAs have questioned the validity of employee consent, as employees do not have a genuine choice, given the imbalance of power in an employee/employer relationship.

Under the GDPR it will be more difficult to rely on consent.

Employers will need to carefully re-assess the legal grounds on which they process employee personal data. If they rely on consent, they will need to check whether they meet all the requirements imposed by the GDPR and bear in mind that free consent implies that it may be revoked at any time.

In many cases, companies will need to move to one of the other legal grounds to (continue to) process employee personal data. This could be contractual necessity (e.g. for the processing of employee payment data), a legal obligation (e.g. for the processing of employee data in relation to social security) or the legitimate interest of the employer (e.g. in the context of employee monitoring). However, their legal grounds all have their restrictions and must be narrowly construed. It may well be that a company will have to stop processing some categories of data, or limit the range of data processed, where it cannot rely on any of the legal grounds for processing laid down in the GDPR.

The processing of employee data may be based on the company's legitimate interest if it is necessary for interests pursued by the employer or by a third party. However, this must be balanced against the interests or fundamental rights and freedoms of the employee.

Member states may allow the processing of personal data to be governed by collective agreements, for example by collective bargaining or works council agreements. In some countries with such employee representation frameworks, works council agreements can provide a reliable and safe way to cover the use of data in the workplace



9.2. Examples of where member states may adopt specific national laws

The Regulation harmonises privacy laws across the EEA. However, member states retain power to adopt their own data protection rules in a number of areas. This means that retailers operating in more than one member state will need to continue to comply with a plethora of rules and obligations.

In summary, and for ease of cross-reference with the text of the GDPR, here are examples most relevant for the retail sector where member states may adopt different data protection rules.

- **Article 6.2.** Processing of personal data for legal necessity purposes.
- **Article 8.2.** Age for consent.
- **Article 80.2.** Issues concerning collective redress.
- **Article 83.9.** Certain issues concerning enforcement and sanctions.
- **Article 87.** Processing of a national identification number or any other identifier of general application.
- **Article 88.** Processing of employee personal data.



THIS CHAPTER COVERED

Companies need to monitor whether the member states where they operate implement specific data protection rules in certain areas.

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

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
Audit	<ul style="list-style-type: none">• 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.• 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.• Consider if there are existing audit processes which can be leveraged to monitor compliance in this area.
Notice and consent	<ul style="list-style-type: none">• Identify and review all existing privacy notices and policies concerning employees and customers. Include all relevant people within the company, legal, compliance, HR, etc.• Review and revise the privacy notices to ensure they comply with the new requirements.• Establish in which countries the notices must be translated.• Establish where consent (explicit and unambiguous) will need to be obtained.• Decide how privacy notices, policies and consents will be provided and tracked (automated or manual process, etc.).• Be attentive to DPA guidance, as they may provide standard formats for notice and consent.
Internal process	<ul style="list-style-type: none">• Identify key internal actors responsible for data processing so that they can be involved in developing new processes.• Identify key senior stakeholders to support the accountability programme and the operational (and cultural) changes required to address the accountability requirements.• Create FAQs that will assist management and the relevant departments in responding to customers' and employees' questions (about operations concerning the collection and processing of their data).

Internal policies	<ul style="list-style-type: none"> • Ensure that there are policies in place for providing access and correction of personal data and the exercise of other individual rights. • Establish procedures to be followed for requesting and providing access and making or rejecting requested corrections. For example, how long does HR have to respond to an access request? If an employee's correction requests are rejected, individuals should be notified and given the reasons why the requested corrections have not been made. • Create guidelines and policies regarding data retention. There may be specific local requirements, concerning for example employee and medical records.
Privacy Impact Assessment (PIA)	<ul style="list-style-type: none"> • Create PIA procedure and templates. • 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?
Security	<ul style="list-style-type: none"> • Review and revise internal data security policies and procedures to ensure they are up to date and fit for compliance with the GDPR. • Create any new policies that are necessary. • Create a data breach response plan.
Training for employees with access to personal data	<ul style="list-style-type: none"> • Create training for employees who have access to personal data (i.e. HR, IT, finance). This is not strictly required under the GDPR but is recommended as good practice.
DPO	<ul style="list-style-type: none"> • Identify if a DPO must be appointed. Decide if there should be one DPO for the whole group or a few local DPOs. • Assess if it is better to appoint an internal DPO among staff, employ someone new, or hire an external consultant. • Set out in detail tasks and duties of the DPO and include them in the appointment contract. • Create budget to provide resources for the DPO. • Publish contact details of the DPO (privacy policy, website) and communicate them to the relevant DPA.
Inventory of databases	<ul style="list-style-type: none"> • Create a new or update existing inventory of databases. • Update or file the necessary notifications with the DPAs, where required. Although the GDPR removes the notification requirement, the notification with the local DPA will be replaced by a requirement to keep internal records. Any work on filings during the next months will be helpful. Companies should also gather the additional details that will be required for the internal records under the GDPR.
Agreements with service providers	<ul style="list-style-type: none"> • Identify and audit existing agreements with service providers who act as data processors. • Update and negotiate amendments, to ensure compliance with the GDPR. • When negotiating new outsourcing deals integrate the GDPR requirements already now.

Certification	<ul style="list-style-type: none"> • Consider appropriate outreach actions, for example to contribute to new codes of conduct and certification mechanisms in conjunction with relevant industry bodies and associations.
Data transfers	<ul style="list-style-type: none"> • Identify what data flows take place with third countries, and what mechanisms exist for these data transfers and assess their validity under the GDPR. • For intra-group data transfers, consider carrying out a BCR gap analysis to determine the practical viability of BCR. • For transfers to third party service providers (e.g. cloud service providers), put in place a flexible contractual mechanism that also covers sub-contracting.
DPA consultation	<ul style="list-style-type: none"> • Determine where consultation with a relevant DPA is required following a Privacy Impact Assessment.



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



and
99%
of which are **SMEs**.



10% of EU's GDP



29 million jobs



or **1 in 7** of all jobs,
many of them
young people.

www.eurocommerce.eu

Follow us on



January 2017