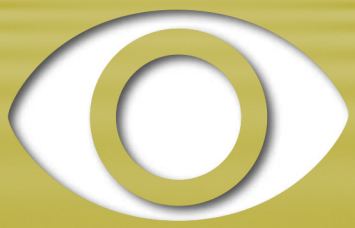
Understanding the GDPR



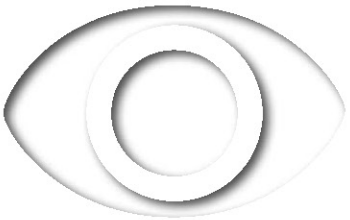
SECO-Institute

Privacy & Data Protection

Foundation Courseware

UNDERSTANDING

the GDPR



SECO-Institute

Privacy & Data Protection

Foundation Courseware

Title
Understanding the GDPR
SECO Institute Privacy & Data Protection Foundation Courseware

Authors
Anna Mácsai, Hans de Vries

Contributors and reviewers
Hans van den Bent
Rion Rijker

Publisher
SECO-Institute

ISBN
9789082978100

Print
First edition, first impression, February 2019

Layout and design
Hike Helmantel

Table of Contents

I Introduction

1 Goal of this Book

Understanding the GDPR provides a structured overview of the EU's General Data Protection Regulation and its main practical implications for individuals and businesses within and outside the EU. Following a brief summary of the Regulation's historical and legal background, the book guides readers through the GDPR's most relevant terms and provisions, analysing the legislative text in a readable style and accompanying the analysis with examples and practical observations.

Each chapter was written with the aim of enabling novice readers to grasp the relevant legal terminology and interpret individuals' and organisations' data protection rights and obligations under the GDPR. In this spirit, we recommend our book to candidates who are preparing for the SECO-Institute's Privacy & Data Protection Foundation examination, and all who would like to acquire a solid understanding of the GDPR.

2 Structure of the Book

The book consists of three parts: this **Introduction (I)**, an overview of the **Historical and Legal Context of the General Data Protection Regulation (II)**, and **The House of Data Protection (III)**.

Part II Historical and Legal Context of the General Data Protection Regulation is divided into two chapters.

Chapter 1 Legal Instruments of the Council of Europe and the European Union provides an overview of the two bodies that have shaped the European data protection landscape, defines core concepts relating to EU law-making, and summarises the structure of EU legal acts.

Chapter 2 The Right to Privacy and the Right to Data Protection in Europe describes the evolution of the right to privacy and the right to data protection in Europe, up to the implementation of the GDPR.

Chapters 1 and *2* are followed by a *Summary* and a short *Test*. These are especially useful for examination candidates.

Part III The House of Data Protection is the actual "body" of the book. As indicated in the title, **Part III** uses a house-shaped model to provide a systematic analysis of the GDPR. The six parts of the House represent the six key building blocks of GDPR-compliance or, in a wider context, the six main steps that need to be taken to create an effective data protection architecture.

Following the structure of the House, **Part III** is divided into six chapters.

Chapter 1: Terms and Scope defines the GDPR's key terms and analyses the provisions that determine how, and to what extent, the GDPR affects an organisation's or individual's activities.

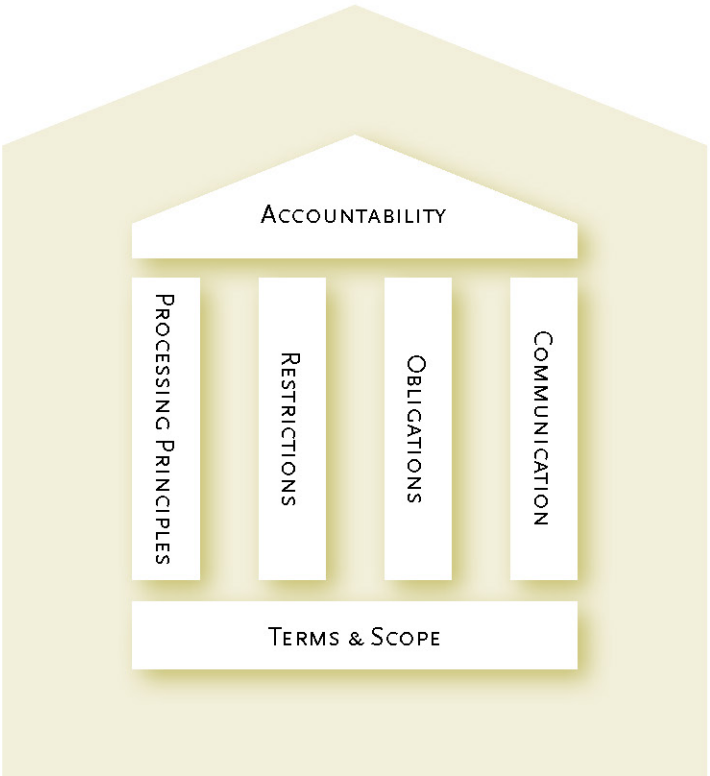
Chapter 2: Processing Principles describes the general principles that govern personal data processing under the GDPR and explains how these principles should be given effect in practice.

Chapter 3: Restrictions covers restrictive provisions and additional considerations that must be taken into account to ensure the compliance of specific processing activities.

Chapter 4: Obligations explains data controllers' and processors' general technical, organisational and administrative obligations.

Chapter 5: Communication outlines data controllers' and processors' communication obligations in the event of a data breach.

Chapter 6: Accountability revolves around the tools that can be used to demonstrate GDPR-compliance.



Within **Part III**, each chapter ends with a *Summary* and a short *Test*.

Finally, the book has four appendices:

— *Appendix I: Answer Key* contains answers for every test in the book, in the order in which they appear in the book.
— *Appendix II: How to Read EU Legal Acts* contains an overview of the structure of EU legislative documents.
— *Appendix III: Table of Contents of the GDPR* contains a list of all GDPR articles linked with the corresponding recitals.
— *Appendix IV: Bibliography* contains a list of references.

3 Examples Used in the Book

With a focus on translating legal provisions into practice, the book illustrates the GDPR's key terms and provisions with examples. In addition to "real-life" examples, the book uses scenarios to illustrate particular issues. The scenarios take place at Bicsma, a fictive company created by the SECO-Institute to provide context for the assignments and case studies used in SECO's educational material.

Bicsma

Bicsma is a Dutch (EU) beverage manufacturer. The company is managed by three brothers: Vincent, Hans and Marcel Bicsma.

Bicsma was launched in the family's kitchen when Ma Bicsma, the family matriarch started producing home-made fruit juices for local supermarkets. The juices were so well-received that Bicsma soon became a medium-sized company with two production facilities and 354 employees.

Bicsma is engaged in both business-to-business and business-to-consumer activities. In a somewhat unusual manner, the company sells drinks to both supermarkets and individuals.

As GDPR-compliance is one of Bicsma's top priorities, the company has recently employed Dana, a new Data Protection Officer.

4 Notes to the Reader

— The book contains references to opinions and guidelines issued by the Article 29 Working Party (WP 29), an independent data protection advisory committee set up by *Directive 95/46/EC*, the GDPR's predecessor. When the GDPR entered into force, the Article 29 Working Party ceased to exist and was replaced by the European Data Protection Board (EDPB). Although the (then) Article 29 Working Party's opinions and guidelines were published under *Directive 95/46/EC*, most of them remain relevant for the GDPR, wherefore they are often cited in this book.

— The summaries and tests included in this book help readers to prepare for the SECO-Institute's Privacy & Data Protection Foundation certification exam. The test questions reflect the content and difficulty of the certification exam but do not fully mimic the format used in the certification exam. The certification exam only contains multiple choice questions.

The House of Data Protection

1 Terms and Scope

Introduction

In order to determine whether, and to what extent, the GDPR affects an individual's or organisation's activities, we first need to understand the Regulation's key terms and provisions relating to four aspects:

— the information the GDPR aims to protect
— the activities the GDPR aims to regulate
— the data protection roles the GDPR defines
— the geographical aspects of the GDPR's applicability

Accordingly, *Chapter 1* is divided into the following four sections:

1.1 Personal Data provides a detailed analysis of the concept of personal data.
1.2 Processing defines the concept of processing and describes the activities that fall within and outside the GDPR's scope.
1.3 Key Data Protection Roles outlines the respective roles, rights and obligations of the actors who are involved in personal data processing.
1.4 Territorial Scope explains in what situations the GDPR applies within and outside the EU.

Chapter 1 Terms and Scope closes with a *Summary* and a *Test*.

1.1 Personal Data

As set out in its Article 1, the GDPR's main objective is to "lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data." In order to determine how the GDPR affects an individual's or organisation's activities, we first need to understand what information the GDPR aims to protect. In other words: we need to understand what information the GDPR considers personal data.

1.1.1 Definition of personal data

Article 4 (1) of the GDRP defines "personal data" as "any information relating to an identified or identifiable natural person (data subject)". This definition might seem discouragingly broad or even unclear. To better understand its meaning, we need to break it down into four building blocks and analyse each block individually.[4]

"Natural person"

The first crucial (maybe self-evident) point in the definition of personal data is that information has to relate to a natural person to qualify as personal data. This has two important implications for the GDPR's applicability. As the law defines "natural person" as a living individual and a real human being, the GDPR's definition of personal data only applies to information that relates to living individuals. This excludes information that relates to deceased persons and "artificial" entities (such as companies and other types of organisations, collectively referred to as "legal persons" in the GDPR). Recital 14 of the GDPR reaffirms that the protection afforded by the Regulation only applies to natural persons – including *all* natural persons, disregarding their nationality or place of residence.

Bicsma

info@bicsma.com is not personal data as it relates to the Bicsma company, not an individual.

vincent.bicsma@bicsma.com is personal data as it relates to an individual (who happens to work at the Bicsma company).

4 The analysis is based on: Article 29 Working Party. 'Opinion 4/2007 on the concept of personal data'.

"Identified or identifiable"

According to the definition of personal data, information relating to a natural person should be considered personal data if that natural person is "identified" or "identifiable".

Article 4 (1) of the GDRP provides a complex definition of "identifiable natural person" or "data subject". According to Article 4 (1), an identifiable natural person or "data subject" is *"one who can be identified, directly or indirectly,* in particular *by reference to an identifier* such as a name, an identification number, location data, an online identifier *or to one or more factors specific to the* physical, physiological, genetic, mental, economic, cultural or social *identity of that natural person"*.

When trying to understand this definition, one will first notice that the GDPR does not define the exact meaning of the term "identify". The Article 29 Working Party's *Opinion 4/2007 on the concept of personal data* clarifies that a natural person should be considered "identified" when they are distinguished from all other members within a group of persons. Accordingly, a natural person should be considered "identifiable" if it is possible to distinguish them from all other individuals within a group of persons.

From the definition of "identifiable natural person", it becomes clear that there are two main categories of information one can use to identify an individual (that is, to distinguish the individual from other individuals): so-called "identifiers" (such as a name or an identification number) and factors that are "specific" to one of the various (physical, physiological, genetic, etc.) aspects of an individual's identity. As the GDPR does not specify what factors should be regarded as "specific" to an individual's identity, this notion should be interpreted as widely as possible. "Specific factor" may refer to any characteristic that relates to an aspect of an individual's identity.

> **Concrete examples of identifiers include names, ID numbers, social security numbers, data collected by mobile devices for navigation purposes, IP addresses and cookie identifiers.**
>
> **Factors that are "specific" to the different aspects of an individual's identity include physical traits (hair colour, eye colour or height), personality traits, preferences, attitudes and beliefs, heritage (ethnicity, nationality, language), sexuality, age category, health conditions, occupation, hobbies, social position, and many other characteristics.**

Depending on the extent to which a piece of information enables us to narrow down the group the individual belongs to and thereby identify the individual, we can distinguish between "direct" and "indirect" identification. Identification should be considered "direct" if a piece of information "obviously reveals" the individual's identity (a typical example of such information is the individual's full name). Conversely, the identification is "indirect" if different pieces of information (such as profession and workplace information) are combined to establish the individual's identity. In the context of the GDPR's applicability, there is no difference between direct and indirect identification. If either direct or indirect identification is possible, the individual should be considered "identifiable".

In theory, any identifier or characteristic could lead to an individual's identification, either directly or indirectly. In practice, however, an individual's identifiability depends on the context of the particular situation. Although full name is usually considered a direct identifier, it would be extremely difficult to look at a country's population and "identify" someone on the basis of a very common first and last name. Likewise, although vocation is commonly regarded as an important aspect of our social identity, it would be impossible to single out an individual from the country's population by solely referring to their profession. At the same time, a common name or a job title may be more than sufficient to identify someone within a business department.

Bicsma

"Vincent Bicsma" is an example of direct identification. Vincent's full name directly refers to a "flesh and bone" individual and thereby allows for the unequivocal identification of that individual. Naturally, if Vincent Bicsma has hundreds of namesakes, other information may be necessary to unequivocally identify Vincent – that is, to distinguish our Vincent from all other Vincent Bicsmas. But even in such a case, Vincent's name would be the starting point for Vincent's identification.

"The Data Protection Officer ... at Bicsma" is an example of indirect identification. As there are many data protection officers and many Bicsma employees, the job title or the company name alone would be insufficient to "reveal" the identity of a specific individual. Yet combining the job title with the company name enables the accurate identification of Dana, Bicsma's Data Protection Officer.

The contextual nature of identifiability raises a new question: How do we decide in a specific situation whether or not a piece of information is sufficient to render an individual identifiable?

Recital 26 of the GDPR states that a natural person's identifiability should be determined based on the "means reasonably likely to be used to identify the natural person". The recital adds that "reasonable" and "likely" means should be interpreted in the context of the available technology, the amount of time required for identification, and the costs incurred. In simple terms: if there are technology tools or any other means that can be used to identify an individual, the tools are available on the market, and the use of the tools would not involve excessive costs and effort, one should assume that a third party (any third party, not just attackers) will use those tools to identify the individual. If this possibility exists, the individual should be regarded as identifiable.

In this approach, personal data is a dynamic concept. Information may or may not become personal data depending on the existence, effectiveness and costs of the tools a third party is able to use to identify the individual about whom the information exists.

> **The GDPR states that dynamic IP addresses are "information relating to an identifiable person" (and therefore personal data) as internet access providers can use logs to identify internet users without making considerable effort or investing too much money in the process.**
>
> **Online aliases should also be regarded as "information relating to an identifiable person" if the individual's identity can be revealed by a simple search.**
>
> **If thousands of persons fill out a general happiness survey on the street only putting their gender on the paper, it would require significant time and effort to identify a particular participant based on the answers and the gender data provided. As the participants cannot be identified with "reasonable" and "likely" means, one may consider them unidentifiable (and therefore, regard their answers as information that does not constitute personal data). By contrast, if the same survey is filled out by the 9 male and 1 female employees of a small enterprise, it would require negligible effort to identify the only female respondent, which would make the answers the individual's personal data.**

The House of Data Protection

2 PROCESSING PRINCIPLES

INTRODUCTION

Having discussed the GDPR's key terms and scope, we will continue with the general principles that govern the processing of personal data under the Regulation.

Article 5 of the GDPR sets out seven general processing principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Chapter 2 is divided into two sections. The first section (*2.1 Understanding the Seven Processing Principles*) explains the seven processing principles and the ways they should be given effect in practice. The second section (*2.2 Lawfulness: The Six Lawful Bases*) elaborates on the six legal grounds based on which personal data may be processed in accordance with the first processing principle, the principle of lawfulness.

Following from the controller's accountability for GDPR-compliance, we will analyse the processing principles from the controller's perspective. This is not meant to imply that compliance with the processing principles is not required from processors.

2.1 Understanding the Seven Processing Principles

2.1.1 Lawfulness, fairness, and transparency

Lawfulness, fairness and transparency are so closely intertwined that they appear as one principle in Article 5 of the GDPR. Yet, in reality, they represent different requirements.

The principle of lawfulness requires controllers to identify a lawful basis (legal ground) for each of their processing activities. Article 6 of the GDPR lists six possible lawful bases that can justify the processing of personal data, allowing controllers to choose the one they deem the most appropriate for the processing activity concerned. The six lawful bases will be discussed in the following section (*2.2 Lawfulness: The Six Lawful Bases for Processing*).

The principle of fairness covers both fair data collection and use, and fair communication with the data subject about the processing. "Fairness" requires the controller to pay particular attention to two factors: the adverse effects the (envisaged) processing activities may have on the data subjects' rights and interests, and the data subjects' reasonable expectations as to how their personal data will be processed by the controller. "Fair" processing implies that the controller strives to minimise potential adverse effects (for example, by limiting the data collection) and does not mislead data subjects about the future use of their personal data.

The data subjects' reasonable expectations are primarily based on their relationship with the controller. In the spirit of "fairness", the controller must not process personal data for any other purposes than the data subjects may reasonably expect based on their relationship with the controller. Another important source of data subjects' reasonable expectations is the information they receive from the controller about the processing. Where the personal data are obtained directly from the data subjects, this information is usually presented in the controller's Privacy Notice. Ensuring that the personal data are only used for the purposes stated in the Privacy Notice (or another document that is intended to inform the data subjects about the processing) and that the document only contains fair terms (see "forced consent" in the following section) are important components of "fairness".

> **For example, a health care centre selling patient data to a multinational company is likely to run counter to data subjects' reasonable expectations, and therefore cannot be considered "fair". Furthermore, processing cannot be considered "fair" if it involves activities of which the data subjects were not informed when the controller obtained the personal data.**

The principle of transparency supports the principle of fairness. Recital 39 of the GDPR states that, in order to be "fair", the controller must make it transparent to data subjects that "personal data concerning them are processed and to what extent the personal data are or will be processed". According to the Article 29 Working Party's *Guidelines on transparency*, "transparency" means that all information coming from the controller is "clear, open, honest, concise, easily accessible, explicit and easy to understand" for the data subject.

To ensure the required level of transparency, the controller must ensure that the information that relates to the processing of personal data (for example, the Privacy Notice) is clearly differentiated from other information that is presented to data subjects (for example, the Terms of Use of a service). Visual transparency is important, as it is not "fair" to force data subjects to search through large amounts of texts in order to find out how their personal data will be processed. Tailoring the information to the target audience (that is, making sure that the information is understood by the average data subject) is also crucial, because "transparency" implies that data subjects are aware of all the risks, rules, safeguards and rights relating to the processing of their personal data. (This becomes especially important when offering services to children.) To ensure that data subjects are truly aware of all data protection risks, rules, safeguards and rights, "transparency" requires the controller to use clear and plain language in its communications with the data subject. This means, in particular, that the controller must use simple sentences that do not leave room for different interpretations. Furthermore, the obligation to use "clear and plain language" means that the controller must refrain from the use of (legal or IT) jargon, avoid the excessive use of auxiliaries (such as "may" and "might"), and be as specific as possible instead of employing vague and broad statements.

> **"We may use your data to offer personalised services" is regarded as unclear language, whereas "We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read" qualifies as clear and plain language.**[21]

As we will see, "fairness" and "transparency" are strongly linked to the data subject's right to be informed and the controller's obligation to inform the data subject about the processing.

21 Article 29 Working Party. 'Guidelines on transparency under Regulation 2016/67'.

2.1.2 Purpose limitation

The principle of purpose limitation states that personal data may only be collected for "specified, explicit and legitimate purposes", and may not be further processed "in a manner that is incompatible with those purposes".

Prior to the processing, the controller must determine the purpose of the processing and specify what is and what is not included within the scope of that purpose. As we will see in the following section, the purpose only becomes legitimate if it is based on one of the lawful grounds set out under the principle of lawfulness. The purposes must be phrased in an explicit manner, which strongly relates the principle of purpose limitation to the principles of fairness and transparency (the personal data are only processed for the purposes that are communicated to the data subject and each purpose is described in clear and intelligible language).

> **Vague or general purposes, such as "improving user experience", "marketing purposes", "security purposes" or "future research" do not qualify as specific purposes under the GDPR. Such purposes are also not transparent and fair, as they do not show data subjects how exactly their personal data will be used and what consequences the processing might entail.**
>
> **"We collect and use your name, address and payment information to deliver the products you have ordered with us and to process invoices relating to your orders. In addition, we collect and use your telephone number to notify you in case of delivery issues" is a specified and explicit purpose.**

The principle of purpose limitation allows personal data processing only for the specific purpose(s) for which the data were collected. Further processing (processing for any other purposes than the ones for which the data were collected) is prohibited, except where the "additional" purposes are compatible with the original purposes or fall under an exception (in line with Article 89, exceptions include "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"). If the purposes are compatible, they can be based on the same lawful ground. The Article 29 Working Party's *Opinion on purpose limitation* states that the compatibility of purposes needs to be assessed on a case-by-case basis, considering three main aspects:

1. The relationship between the purposes: there should be a connection between the original purpose and the additional purpose.

2 The context of the processing, including the reasonable expectations of the data subject (the additional purpose must be compatible with the data subject's reasonable expectations based on the data subject's relationship with the controller and the controller's communications towards the data subject).
3 The nature of the personal data, the foreseeable impact of the further processing, and the safeguards applied by the controller.

If the analysis shows that the additional purpose is not compatible with the original purpose, the controller must specify the additional purpose as a "new" purpose and base the new purpose on its "own" legal ground.

Bicsma

A customer asks Bicsma to deliver him a selection of fruit juices every week. In the strict sense of purpose limitation, this means that Bicsma "further processes" the customer's personal data every week, as the original purpose was to deliver the first order. Although each delivery can be regarded as "processing for an additional purpose", it is more than obvious that each additional purpose is compatible with the original purpose. There is a connection between the purposes (the goal is to deliver products ordered by the customer), the processing is in line with the data subject's expectations, and each processing activity has the same foreseeable impact.

If Bicsma sends a delivery satisfaction form to the same customer's e-mail address, the new purpose (measuring customer satisfaction) might be related to the original purpose (juice delivery), but the purposes do not fully match. Bicsma may ask for the DPO's advice to decide whether the purposes may be considered compatible, or make "measuring customer satisfaction" a new purpose and base the new purpose on its "own" lawful ground.

Using Bicsma customers' personal data to detect whether they are using an Apple computer or a Windows PC in order to offer greater discounts to Windows users, would be clearly incompatible with the original purpose of the processing. Such use of customer data would also violate the principle of fairness, as it would exceed customers' reasonable expectations as to how their personal data will be processed by Bicsma.

2.2 Lawfulness: The Six Lawful Bases

The principle of lawfulness requires the identification of a lawful basis (legal ground) for every processing activity performed by the controller or on behalf of the controller. Article 6 of the GDPR identifies 6 lawful bases as valid legal grounds for the processing, allowing controllers the freedom to choose the most suitable one for each processing activity. This section provides an overview of the lawful bases and the factors that come into play when deciding which lawful basis is the most appropriate for a specific processing activity.

2.2.1 The data subject's consent

"the data subject has given consent to the processing [...] for one or more specific purposes"

Obtaining the data subject's consent might seem the easiest way to ensure compliance with the lawfulness principle: the controller asks for the data subject's permission to process their personal data and the data subject grants that permission, giving a green light to the processing. In practice, however, relying on the data subject's consent has complex implications as consent needs to meet strict requirements to be recognised as a valid ground for processing.

To begin with, consent must be "freely given", which means that providing consent must be truly optional for the data subject. As set out in Recital 43 of the GDPR, this condition is not met in situations where there is a "clear imbalance of power" between the controller and the data subject. In an employee-employer relationship or in an individual's relationship with the public authorities, consent cannot be a lawful basis as the individual is not completely free to refuse it. The same applies to situations where the controller requires the data subject to provide consent to the processing in exchange for a service, in spite of the fact that the processing would not be absolutely necessary to provide that service. Recital 42 of the GDPR reasserts that consent is not truly optional and, therefore, does not constitute a valid ground if the data subject is unable to refuse consent without being disadvantaged: "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment." This suggests that consent may only be used as a lawful basis if it can be ascertained that the data subjects who refuse consent have the same opportunities as those who provide consent, unless the processing relates to a service that cannot be provided without acquiring the data subject's consent.

The complexity of the "consent issue" is reflected in the many criticisms levelled at Google's, Instagram's, WhatsApp's and Facebook's privacy practices. Max Schrems, an Austrian lawyer and privacy activist filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook in May 2018. The complaints argue that the tech giants "blackmail" users into accepting their data collection policies by only offering them two options: they either consent to the processing of their personal data (including use for targeted marketing purposes), or they stop using the service.

In addition to being "freely given", consent must be "specific, informed and unambiguous". This means that consent has to be given for a specific purpose and the data subject has to be aware of this purpose as well as the identity of the controller. Recital 32 of the GDPR adds that consent must be given by a "clear affirmative act"; in other words, it must be something the data subject has said, written or done to indicate that they agree to the processing of their personal data.

Signing a form or ticking a box are examples of a "clear affirmative act", whereas silence, inactivity or failure to opt out do not qualify as clear affirmative acts.

Controllers relying on the data subject's consent as a lawful basis must ensure that their data subjects know exactly what they are consenting to (what personal data will be processed by whom and for what purposes), and that the data subjects have the option to refuse consent without being deprived of opportunities that are available to those who consent to the processing. These requirements often represent a challenge for cookie statements. If accepting cookies is a prerequisite to using a website (think of "By using this site, you accept cookies"), consent is not valid as the data subject has not been given the opportunity to refuse consent without detriment (the only options are to accept the cookies or not view the website). Vague statements ("We use cookies to provide you with a better service") also render consent invalid, as they are not specific and informative. A GDPR-compliant cookie statement should at least inform data subjects of what cookies are used for what purposes, which of them are essential for the functionality of the website, and which cookies can be opted out of.[22]

22 Cookies are also addressed in the ePrivacy Directive (Directive 2002/58/EC), which will soon be replaced by the ePrivacy Regulation.

Bicsma

Here is Bicsma's cookie statement. (Note that this is a simplified example).

This website uses cookies

We use cookies to personalise content, to analyse our traffic, and to personalise our ads.

✓ Necessary
❑ Statistics
❑ Marketing

Details

About cookies

Necessary (1)

Necessary cookies enable basic functions, like page navigation. The website cannot function properly without these cookies.

Name	Provider	Purpose
Cookie	bicsma.com	log-in

Statistics (1)

Name	Provider	Purpose
Cookie	bicsma.com	Registers a user ID to generate statistical data on how the visitor uses the website.

Marketing (1)

Name	Provider	Purpose
Cookie	bicsma.com	Personalises ads based on your preferences.

On account of several further rules, the data subject's consent is often regarded as the least favourable lawful basis for personal data processing. In particular, there are four additional aspects controllers should consider before choosing consent as a lawful basis:

1 Consent has to be given for one or more specific purposes. This implies that the controller has to seek new consent from its data subjects every time it intends to process the personal data for a new purpose. In many cases, this is quite difficult.

2 The data subject has the right to withdraw consent any time (see *Chapter 3 Restrictions*). If the data subject withdraws consent to the processing, the controller must cease the processing of the personal data and demonstrate that the data subject's request has been granted.

3 The controller must be able to demonstrate that it has obtained the data subject's consent. This implies that the controller must document when, by whom and for what purpose the consent was given – which, again, may be a quite burdensome obligation.

4 The use of consent may be subject to further restrictions depending on the categories of the personal data concerned and the age of the data subject (see *Chapter 3 Restrictions*).

Taking note of all the difficulties consent implies, controllers may decide to rely on one of the other 5 lawful bases.

2.2.2 Contractual obligations and pre-contractual steps

"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

This lawful basis applies where there is a contract between the controller and the data subject or when the data subject wishes to enter into a contract with the controller, and the processing is necessary to perform the contract or to take the desired pre-contractual steps. When relying on "contract or pre-contractual steps" as a lawful basis, the controller must carefully assess whether the personal data are truly necessary for the purposes of performing the contract or taking the pre-contractual step. If the controller can perform its side of the contract or take the pre-contractual step without processing the personal data, the personal data should not be processed. If the controller deems that the processing is essential for the contract or the pre-contractual step, it should justify and document this decision to prevent difficulties in the future.

> **Typical examples of processing activities that rely on this legal basis are activities performed in the context of employment. Before an employment contract is drawn up, employers may need to verify whether the applicant has the right to work in the country of employment. This is a pre-contractual step, for which employers need to process certain categories of personal data. To perform their part of the employment contract (to pay salaries), employers need to process their employees' bank account details.**

Summary: Processing Principles

"The principles of data protection should apply to any information concerning an identified or identifiable natural person."

Recital (26)

Principles relating to processing of personal data

1 **Lawfulness, fairness, and transparency**
2 **Purpose limitation**
3 **Data minimisation**
4 **Accuracy**
5 **Storage limitation**
6 **Integrity and confidentiality**
7 **Accountability**

Article 5

The Principles are an important cornerstone of the GDPR.

The GDPR lists the seven principles in Article 5, and elaborates on "lawfulness" (the lawful bases) in Article 6.

Lawfulness, fairness, and transparency

Lawful: legal basis for processing (discussed in detail in Article 6).
Fair and transparent: informing the data subject about the processing in clear and understandable language, without withholding information, and striving to reduce potential adverse impacts.

Purpose limitation

Collected for specified, explicit and legitimate purposes.

— specified: specific purpose, not vague
— explicit: purposes are "revealed and explained using clear and plain language"
— legitimate: processing must be based on one of the legal grounds stated in Article 6

Data minimisation

Adequate, relevant and limited to what is absolutely necessary to fulfil the purposes for which the data are processed.

— ask yourself if you really need the personal data to fulfil your purpose ("Are there other ways to achieve the purpose?")

Accuracy

Accurate (in the light of the purpose for which processed) and, where necessary, kept up to date.

— take every reasonable step to erase or rectify inaccurate personal data without delay

— check accuracy on a regular basis (importance depends on the purpose of the processing, the nature of the personal data, and the impact on the data subject's rights and interests)

Storage limitation

The period for which the personal data are stored (retention period) is limited to "a strict minimum", in light of the purposes of the processing.

— the controller should perform periodical reviews

— for certain data categories, retention periods may be set by national law (for example, retention of financial information for tax purposes)

Integrity and confidentiality

Processing personal data in a manner that ensures the appropriate protection of the data against unauthorised or unlawful processing and against accidental loss, destruction or damage

— this must be achieved by "using appropriate technical or organisational measures", such as pseudonymisation, encryption, identity & access management or clean desk policies.

Accountability

The accountability principle requires compliance with the processing principles and obliges the controller to be able to demonstrate compliance.

Lawfulness of processing

1 Consent
"the data subject has given consent to the processing of his or her personal data for one or more specific purposes"

2 Contractual and pre-contractual obligations
"the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

3 Legal obligations
"the processing is necessary for compliance with a legal obligation to which the controller is subject"

4 Vital interests
"the processing is necessary in order to protect the vital interests of the data subject or of another natural person"

5 Public interest or official authority
"the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

6 Legitimate interests of the controller
"the processing 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 data subject which require protection of personal data, in particular where the data subject is a child"

Test III/2: Processing Principles

Question 1

Which processing principle requires the controller to specifically describe what the personal data will be used for?

A Accuracy
B Accountability
C Purpose limitation
D Integrity and confidentiality

Question 2

Bicsma wants to hire a designer to create the company's new corporate house style. Candidates are required to have a Bachelor's degree in an Art & Design. The HR manager is using candidates' social media sites to gather extra information about their families. The manager wants to see if "art is in the candidates' blood".

Does this processing activity comply with the principle of data minimisation? Why/why not?

Question 3

An ambulance service reacts to an emergency call concerning a motorway accident. One of the unconscious victims needs a blood transfusion. The ambulance crew requests access to the patient's medical dossier.

Is the processing lawful? Why/why not?

Question 4

When the GDPR came into effect, many web shops and online service providers sent out e-mails asking users to consent to the processing of their personal data. The e-mails warned that users who refuse consent would not be able to view online brochures or place orders.

What is wrong with asking for consent this way?

Question 5

In which case are the controller's legitimate interests likely to override the data subject's rights and interests?

A The controller processes the personal data in order to defend a legal claim.
B The controller processes the personal data for direct marketing purposes.
C The controller processes the personal data to assess customer satisfaction.

Understanding the GDPR

Understanding the GDPR is a comprehensive textbook intended for all those who aspire to develop a solid understanding of the EU's General Data Protection Regulation and its implications for individuals and businesses within and outside the EU.

The book analyses and explains the GDPR's terminology and provisions in clear terms and in an engaging way, connecting theory to practice with real-life examples and fictitious scenarios. To support durable learning, the chapters are accompanied with summaries, practice tests and answer keys with detailed answer explanations.

The book was specifically designed to prepare candidates for the SECO-Institute's Privacy & Data Protection Foundation exam, but it is an excellent resource for anyone who strives to gain a full picture of rights and obligations under the GDPR.

About the SECO-Institute

The SECO-Institute is a leading provider of data protection, information security, IT security and business continuity trainings and qualifications. The Institute's mission is to train highly competent professionals in the protective disciplines and to enhance the quality of cybersecurity education through coherent and practical training programs.

The Privacy & Data Protection Foundation training is the first level of the SECO-Institute's Certified Data Protection Officer certification track.

SECO® INSTITUTE

9789082978100