PRIVACY AND DATA PROTECTION BASED ON THE GDPR

UNDERSTANDING THE GENERAL DATA PROTECTION REGULATION

Leo Besemer

Van Haren PUBLISHING

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT and IT Management
- Architecture (Enterprise and IT)
- Business Management and
- Project Management

Van Haren Publishing is also publishing on behalf of leading organizations and companies: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, CATS CM, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur
Methode
TOGAF®

Business Management

BABOK® Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
CATS CM®
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

Project Management

A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net.

Privacy and Data Protection based on the GDPR

Understanding the General Data Protection Regulation

Leo Besemer

Van Haren PUBLISHING

Colophon

Title:	Privacy and Data Protection based on the GDPR
Subtitle:	Understanding the General Data Protection Regulation
Author:	Leo Besemer
Text editor:	Steve Newton (Galatea)
Publisher:	Van Haren Publishing, 's-Hertogenbosch, www.vanharen.net
ISBN Hard copy:	978 94 018 0676 3
ISBN eBook pdf:	978 94 018 0677 0
ISBN ePub:	978 94 018 0678 7
Edition:	First edition, first impression, September 2020
Cover illustration:	Isabella de Felip
Layout and DTP:	Coco Bookmedia, Amersfoort – NL

Foreword

Chapter 1 of "*Privacy and Data Protection based on the GDPR*" describes how in 1890 the Boston lawyer and future U.S. Supreme Court Justice, Louis Brandeis, together with his partner Samuel Warren, published in the Harvard Law Review a classic article – "The Right to Privacy". A key topical concern of Brandeis and Warren was the first introduction to consumer markets of portable and cheap cameras and their potential use by 19th century paparazzi to harm people's confidentiality. In other words, the main issue which triggered their article was technological development resulting in abuse of the individual's right to privacy – plus ça change …

The right to privacy was included in the European Convention on Human Rights drafted in 1950. It created an essential human rights standard which is binding on the Council of Europe members. The consistency it introduced to Europe is highly important. For instance, when comparing privacy rights in Irish and English law, Article 40.3.1 of the Constitution of Ireland adopted by a vote of the people in 1937 provides that "the State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen". The courts have held that one of these personal rights is the Irish citizen's right to privacy.

On the other hand, in Kaye v Robertson [1991] FSR 62, it was stated by Lord Justice Glidewell that "it is well known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy". Both countries have subsequently incorporated the Convention rights – including the Article 8 right to privacy – into national legislation. And another vital point is that these are "human" rights – rights we all have by virtue of our common humanity and not because of our citizenships, or the jurisdictions in which we reside. Likewise, our right to the protection of our personal data under European Union law provides a shared standard for and across all Member States.

Although there is significant overlap between our right to privacy and our right to protection of our personal data, they are not identical. This is often misunderstood – privacy and data protection are frequently thought to be 100% synonymous. But as Leo points out, they are separate and distinct rights under the Charter of Fundamental Rights of the European Union. Similarly, the Council of Europe has its Convention on Human Rights, separate from its more specific Convention 108+ for the protection of individuals with regard to the processing of personal data.

To demonstrate, Article 5 of the GDPR sets out six basic principles for the application of our data protection rights. And, for example, a failure to adhere to the obligation under Article 5(1)(f) for securing personal data from "accidental loss" is not, per se, an infringement of privacy. However, a data protection failure resulting in accidental loss, e.g., of a hospital patient's medical records, could have potentially fatal consequences – there can be nothing more serious.

This highlights a key theme of the GDPR – taking appropriate account of the risks to data subjects resulting from failures to protect their personal data. Part IV – "Risks assessment and mitigation" – covers this very well. The word "risk" appears eight times in the English language text of data protection Directive 95/46/EC, compared to 75 times in the GDPR. However, this is very frequently ignored by organizations. This was plainly shown to me by a survey I did in 2019 of data protection officer (DPO) recruitment advertisements throughout Europe. DPOs are required under Article 39(2) to take a risk-oriented approach to the performance of their tasks. The implication is that risk assessment and management is an essential component of the DPO's expertise. But in my survey this risk expertise was neither required by, nor desirable for, 76% of employers.

It is also important to emphasize that although the six basic GDPR principles are legal obligations, they also provide a first-rate framework for the data management and governance described in Chapter 6. So, even if not required to, it would still be in every organization's interests to apply them. An obvious illustration is the Article 5(1)(d) requirement to keep personal data accurate and up-to-date. However, to the extent that our organizational decisions are based on data which is inaccurate or out of date, they will be flawed and less effective. Therefore, we clearly should be doing this anyway.

In order for organizations to reach a good compliance standard with the data protection principles, it must be absorbed into organizational culture from top to bottom. Under GDPR Article 38(3), DPOs must "directly report to the highest management level". This infers that, firstly, the highest management must have a reasonable understanding of what is being reported to them and, secondly, that data protection compliance must be carried out as a strategic issue. Leo's book can provide very effective support to you and your colleagues in reaching this understanding and applying it in practice.

Fintan Swanton,

LLM MSc CEng FICS MBCS.

Senior Data Protection Consultant & Managing Director,
Cygnus Consulting Ltd.

www.cygnus.ie

Fintan Swanton is the Irish representative in the Confederation of European Data Protection Organizations (CEDPO).

Contents

Acknowledgements

While writing this book, people in my neighborhood asked me “isn’t it incredibly boring to write about privacy law?” Others told me about the misconceptions they had seen in the companies and organizations where they work: “People seem to think that everything is different now, or even that everything they need to do is now illegal.” You can hear the same message in TV news: “Government organization X cannot function properly because of the limitations imposed by privacy law” and “Errors in the healthcare sector because patient data may no longer be exchanged, while this is urgently needed”.

For me it was a pleasure to write this book, and no, it is not boring. On the contrary, the more I studied the details to try and make it a clear and comprehensible story, the more interesting it became.

But this book is not an effort of one solitary person in a silent room, somewhere in the rural north of the Netherlands. That is how it started, a lot of text based on an earlier white paper and some blog articles I wrote for EXIN. After those first steps, however, it became a team effort.

Acknowledgements to Marianne Hubregtse and Rita Pilon of EXIN for the idea to write this book, to Ivo van Haren and Bart Verbrugge of Van Haren Publishing for good counsel and excellent critiques, to Fintan Swanton for kindly providing a perfect foreword, to Steve Newton for correcting the many errors and imperfections in the English text I wrote. If you still find an infringement on English spelling or grammar, it is certainly mine.

How this book is organized

For many organizations processing personal data, the General Data Protection Regulation (GDPR) came as a shock. Not so much its publication in the spring of 2016, but rather the articles that appeared about it in professional journals and newspapers leading to protests and unrest. "The heavy requirements of the law would cause very expensive measures in companies and organizations", was one of the concerns. In addition, the "173 recitals and 99 articles left too much room for interpretation, while companies which failed to comply would face draconian fines".

This book is intended to explain where these requirements came from and to prove that the GDPR is not incomprehensible, that the principles are indeed remarkably easy to understand. However, the other points cannot completely be denied. The regulation forces companies to upgrade their data governance to a level where their data, in particular their personal data, is safe and the rights and freedoms of the data subjects involved are protected. And for those companies and other organizations that don't even try to comply, the fines imposed *should be effective, proportionate and dissuasive*, to quote GDPR Recital (151).

Part I of the book covers the history of privacy and data protection, amongst others showing that the "new" requirements of the GDPR were not that new at all. The material and geographical scope of the GDPR is explained, including how the GDPR interacts with, and is complemented by, other EU and national law. For example, when a type of processing falls outside the scope of GDPR, it does not necessarily mean there is no harmonized framework of national law that covers it.

Part II is the backbone of this book. We start with the main characters. Who are those 'stakeholders'? Who is responsible, who is accountable and for what exactly? What responsibilities, duties, rights and obligations are associated with the role they have? The controller, responsible and accountable for compliance with the GDPR, including the implementation of the principles of personal data processing and the principles of data protection by design and by default. The processor, processing personal data on instruction of the controller, but unlike before also responsible for their own compliance to the GDPR. And the data protection officer as an independent advisor, facilitating a seamless merger between the company's interests and compliance to the GDPR.

We then move on to the practical side of things. The principles for processing personal data are included in Chapter 3, requiring amongst others that processing shall be lawful. Chapter 4 details the six lawful grounds for processing. Chapter 5 covers the rights of the data subject, the individual whose personal data is to be processed. That includes what kind of requests executing those rights an organization should expect and how to deal with those requests in an effective and efficient manner.

Chapter 6 deals with data governance, with methods to responsibly deal with the valuable data of an organization within the requirements set by the GDPR. The last chapter of this part, Chapter 7, examines modern techniques such as tracking and tracing for the collection of personal data and its further processing, and the area of tension between, on the one hand artificial intelligence and machine learning, which form the basis for valuable services and, on the other hand, the requirements set by the law to protect the citizen whose personal data is required for this.

Part III deals with international transfers of data. The concept of data transfer and the rules regarding hiring processors in third countries. The protection of individuals in the EEA from risks of controllers processing their data through websites based in third countries, and of storage in the cloud, which in practice may amount to a server park somewhere in a distant country. And the rules for transfers within the EEA and from the EEA to third countries, including data transfer to the USA and the United Kingdom.

Part IV is about assessment of the risks of processing and also mitigating those risks. Chapter 10 details the data processing impact assessment (DPIA), assessing the risks to the data subjects and their data caused by a processing operation, but also the risks for the organization. Chapter 11 covers data breaches and mitigating the consequences of such a security incident, including the mandatory procedures on investigation and notification.

Part V covers the framework of supervisory authorities (DPAs), each monitoring implementation of the GDPR in their own territory but also cooperating strongly to maintain harmonization. Their legitimate basis, competencies, tasks and powers. The role of the DPA in enforcement: inspections, warnings and administrative fines.

In this book I refer to a "supervisory authority" as the concept of an authority overseeing international cooperation, and to "data protection authority" (DPA) as the national (or regional) institution with its tasks and responsibilities. In the context of the GDPR there is no real difference between the terms mentioned here.

The **Appendices** contain sources and references. The literature used in writing this book and for further reading, among them the publications of the EDPB, extensively detailing the concepts and articles of the GDPR. And there is an index to help you find the topics you are looking for.

References to the GDPR

In this book I will often provide references to the General Data Protection Regulation, both in footnotes and by quoting parts of the legal text, like this:

1. Personal data shall be:
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   (b) collected for specified, explicit and legitimate purposes (...)

GDPR Article 5

In a footnote, and indeed also in other literature on this topic, the second sentence of the article quoted above would be referred to as GDPR Article 5(1)(a), which is pronounced as Article 5, paragraph 1, subparagraph a. The ellipsis (…) in the second subparagraph is to indicate that the quote does not contain the complete GDPR article. GDPR Article 5 actually consists of two paragraphs, of which the first paragraph is subdivided in six subparagraphs (a through f).

Preceding the 99 articles, the GDPR also contains 173 recitals:

Whereas:
(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

GDPR Recital (1)

This (first) recital of the GDPR would be referenced to as GDPR Recital (1), with (Arabic) figures enclosed in brackets. The recitals are a very important part of the GDPR, as they provide context and explanation of the meaning of the articles. You cannot fully understand the meaning of the articles, their intention, scope and reach, without taking the corresponding recitals into consideration. Unfortunately, the text of the GDPR does not indicate which recitals a specific article relates to. One must read through the whole document to see the connections. Or take the better alternative: read this book.

PART I | Privacy and data protection history and scope

In this first part of the book we look into the history of privacy and data protection law. The need for privacy has increased tremendously over the past century, fueled by advancements in technology that offer ever more opportunities to collect information about individuals. The concept of privacy as a fundamental right was only established after, and undoubtedly also as a result of, the Second World War. Chapter 1 describes how the right to privacy was incorporated in treaties and later in law, and how this ultimately led to the General Data Protection Regulation (GDPR) which is applicable law in the EU and the Member States of the European Economic Area.

We then move on to the context in which the GDPR interacts with other European law and with national law in the Member States. We sometimes tend to forget how much legislative power we have given to the EU. Based on the *Treaty on the Functioning of the European Union (TFEU),* however, the GDPR as a European regulation not only interacts with national law, it *supersedes* it.

The GDPR is very important for anyone who processes personal data on European residents in any way, but the scope of the law is not unlimited. That is what the rest of Chapter 1 is devoted to. Questions like "can we still send season's greetings" and "what about the rowing club's list of members" are answered there.

1 History and context

Key subjects

In this chapter we will cover:

- The history of privacy as a concept;
- Privacy and data protection from a legal viewpoint;
- Applicable European and national law regarding privacy and data protection;
- The scope of the General Data Protection Regulation.

1.1 The history of privacy and data protection

At the time our distant ancestors lived as nomads, privacy was not an issue. In fact, it was in the group's interest to stay close at all times, to hunt together, to look out for the group and help defend it, to share food, shelter and indeed body warmth. Knowing each other intimately was important, both because of the need to trust each other's skills and to be aware of hostile intentions, such as the continuous struggle for leadership of the group. In those circumstances, seeking isolation would be seeking danger and being banned from the group would almost certainly lead to death.

This lack of personal privacy did not really change in the ages thereafter. Poor people had little or no privacy, either because they were not free (slaves, serfs, servants, etc.) or because they lived closely together in settlements or neighborhoods where the same need for mutual help and support still existed. But the rich had hardly any privacy either, because the habits and the necessity of security required the continuous presence of many staff. Seclusion was seen as abnormal behavior. The view was that you would only seek it if you had something to hide. Only if you wanted to do something that could not bear the light of day.

The need for privacy as we know it today came up for the first time at the end of the 19th century, when newspapers appeared with extensive society pages, taking gossip to a new level. The announcement on 22 October 1882 of the engagement of Mr. Samuel D. Warren Jr. and Miss. Mabel Bayard, was a kind of starting point. Samuel Warren was a young lawyer from Boston, USA, and as such not used to being the subject of newspaper headlines. His fiancée, however, was a daughter of Senator Bayard and what we today would call a celebrity. Over the following decade, more than sixty newspaper articles appeared, describing down to the smallest detail their social life, their marriage, their family's highlights and sad events. (Gaida 2008).

The continuing intrusive press coverage ultimately lead to an article in Harvard Law Review, written by Louis D. Brandeis and Samuel D. Warren Jr. (Brandeis 1890), which is widely regarded as the first publication in the United States to advocate a right to privacy.

"The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle." (...)

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.'"

"Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops. (...)"

Source: (Brandeis, 1890)

In the article Warren and Brandeis advocate the necessity of law enforcing this right to be let alone and describe its boundaries as an extension of the then existing common law. At that time privacy was thought of as a relational matter, only existing in the context of home and family. At first, however, this desire to control personal information and social image, and the plea for a legal system to protect these rights, did not get much attention.

Up to and directly after World War II, state constitutions protected only aspects of privacy. Such guarantees concerned, for example, the inviolability of the home and of correspondence and the classical problem of unreasonable searches of the body. No state constitution, however, contained a general guarantee of the right to privacy. An integral guarantee protecting the more specific aspects of privacy and private life in their entirety, was unknown at the time.

1.1.1 Human rights law

1.1.1.1 Universal Declaration of Human Rights

After World War II, the UN Commission of Human Rights (UNCHR) started working on what was initially intended as an *International Bill of Rights*. It was one of the first attempts to make globally enforceable agreements. EU history literature (Diggelman, 2014) describes the tedious discussions between the members of the Committee, representants with very different legal and cultural backgrounds from all regions of the world. This was a time when the right of women to be treated as equals to men was hardly accepted anywhere, a time when governments all over the world had come to regard torture and inhuman treatment as acceptable means to an end.

The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. The UDHR was proclaimed by the United Nations General Assembly in Paris on December 10, 1948 (General Assembly resolution 217A) as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected. In its preamble the UDHR recognizes that "*the inherent dignity and (…) the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world."*

The declaration explicitly defines the right to a private life and the freedoms associated with this:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.
> Everyone has the right to the protection of the law against such interference or attacks.
>
> UDHR Article 12

However, the declaration also defines the right to freedom of information and expression:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
>
> UDHR Article 19

These provisions may seem at odds, in particular where the exercise of the rights defined in Article 19 might result in an invasion of privacy, violating Article 12. This potential conflict, however, is reconciled later:

> In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.
>
> UDHR Article 29(2)

Keeping the balance between the right to information and the rights and freedoms of individuals, however, is a challenge. A thread through the history of privacy law up to the current day.

It took another eighteen years before the United Nations in UN Assembly Resolution 217 (III) agreed upon the *International Bill of Human Rights,* consisting of the *UDHR*, the *International Covenant on Civil and Political Rights* (ICCPR, 1966) and the *International Covenant on Economic, Social and Cultural Rights* (ICESCR, 1966). The two covenants

entered into force in 1976, after a sufficient number of countries had ratified them. The covenants require countries ratifying it to include the principles described in them into their national legislation.

The provision of ICCPR Article 17 of is almost identical to Article 12 of UDHR, but the word *unlawful* has been added twice:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honor and reputation.
>
> ICCPR Article 17

The amendment changes the concept of the right to privacy in the sense that governments have the right to intrude on a person's privacy for reasons explicitly laid down by law.

1.1.1.2 European Convention on Human Rights

In the aftermath of World War II, a strong need was felt for European co-operation. Many pro-European movements actively promoted the establishment of an organization that would prevent a return to totalitarian regimes and would defend fundamental freedoms, peace and democracy. On 5 May 1949, the Council of Europe was founded in London. Its aim, according to Article 1 of its statute, is "*to achieve a greater unity between its Members for the purpose of safeguarding and realizing the ideals and principles which are their common heritage and facilitating their economic and social progress*". An important role of the Council of Europe is to promote human rights through international conventions. One of the first of these was the Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights (ECHR), which entered into force on 3 September 1953.

Figure 1.1 COE logo.

From the original ten members in 1949, today the Council has grown to 47 members, including all members of the European Union. The map in Figure 1.2 shows the current Member States of the Council of Europe.

Note that Belarus is not a member, because the country does not meet the human rights and democratic standards of the Council. In particular, it will have to abolish the death penalty if it wants to join.

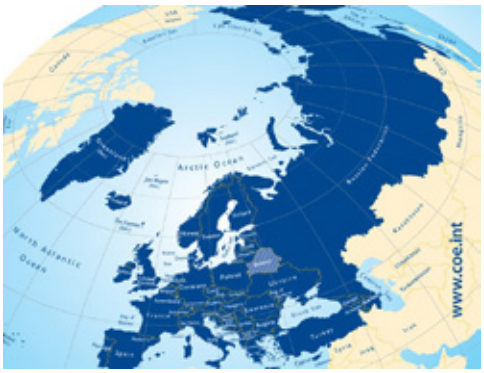

Figure 1.2 Council of Europe Member States.

The ECHR is important because of the scope of fundamental freedoms it protects. These include the right to life, prohibition of torture, prohibition of slavery and forced labor, the right to liberty and security, the right to a fair trial, no punishment without law, the *right to respect for private and family life,* freedom of thought, conscience and religion, freedom of expression, freedom of assembly and association, the right to marry, the right to an effective remedy and the prohibition of discrimination.

With regard to privacy and data protection, the ECHR includes the text of the UDHR:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

ECHR Article 8

In the ECHR, just as in the ICCPR, this protection of the rights of individuals is not absolute. There may be lawful reasons of public interest for governments to breach an individual's right to privacy. Just as the UDHR does, the ECHR recognizes that there is a need to balance the rights of individuals with *justifiable* interferences with these rights.

The importance of this text as a part the European Convention is that it is now part of a treaty to uphold human rights throughout the Member States of the Council of Europe. New members of the Council are expected to ratify the ECHR and other Council of Europe treaties at their earliest opportunity. The ECHR is also a significant and powerful legal instrument because it is enforced by the European Court of Human Rights. The rulings of the Court are binding on the Member States concerned.

1.1.1.3 OECD Guidelines and the Treaty of Strasbourg

In the 1970s, the progress in data processing and the increased possibilities in the use of telecommunications lead to concerns that Article 8 of EHCR was no longer sufficient to protect "*the right to respect for his private and family life, his home and his correspondence*". Large mainframes were introduced allowing big companies and public administrations to improve the collection, processing and sharing of the personal data of millions of people, using large databases. As a result, a need was felt for new standards that would allow individuals to exercise more control over their personal information. At the same time, international trade required the free international flow of information. The challenge was once again to find a balance between these aims.

A new effort to reconcile the protection of privacy and the need for free international flow of personal data came from the Organization for Economic Co-operation and Development

(OECD). This organization, founded on 30 September 1961, aims to promote policies designed to achieve the highest sustainable economic growth and employment, and a rising standard of living in member as well as non-member countries, while maintaining financial stability, and thus to contribute to the development of the world economy.

Figure 1.3 OECD logo.

In 1980, the OECD developed the *"Guidelines on the Protection of Privacy and Trans-border flows of Personal Data",* providing basic rules concerning the protection of personal data and privacy and on cross-border data flow. The aim was to help harmonize the data protection laws between countries. The Guidelines were not legally binding, but intended as a basic framework for national data protection law worldwide, introducing the set of data protection principles that we find today in GDPR Article 5. These principles will be discussed in detail in Part II of this book.

1.1.1.4 Council of Europe (CoE) Convention 108

The OECD guidelines were formalized in 1981 in Council of Europe Convention 108, the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, which made it the first legally binding international instrument to set standards for the protection of personal data, whilst at the same time again aiming for a balance with the need for a free flow of personal data for international trade purposes. Convention 108 is also known as "the Treaty of Strasbourg", but due to the place of Strasbourg in European history there are many treaties by that name. Convention 108 came into force on 10 October 1985, after the required five Member States had ratified it. By today, 55 countries have ratified the treaty, among them eight non-members of the Council of Europe.

A weakness in Convention 108 proved to be that it did not provide for transfers of personal data to countries that had not signed Convention 108. This was addressed in 2001 with the *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.* (CETS 181). This additional protocol introduced independent supervisory authorities in each country that signed it, and included the concept of an 'adequate' (in contrast to equivalent) level of protection for cross-border personal data transfers to non-EU countries.

It should be noted that CoE Convention 108 is still binding for states that have ratified it. Over the years, the European Court of Human Rights (ECtHR) has ruled that personal data protection is an important part of the right to respect for private life (EHCR Article 8), and has been guided by the principles of Convention 108 in determining whether or not there has been an interference with this fundamental right.

In 2012 Convention 108 was modernized after public consultations, including reinforcements to the protection of privacy in the digital arena. The modernization process was completed with the adoption of a protocol amending Convention 108 (Protocol CETS No. 223).