GDPR considerations in e-contracts

Vasiliki Monika Pontikidou

UNIVERSITY CENTER OF INTERNATIONAL PROGRAMMES OF STUDIES
SCHOOL OF HUMANITIES, SOCIAL SCIENCES AND ECONOMICS

A thesis submitted for the degree of
LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation

February 2024
Thessaloniki – Greece

Student Name: Vasiliki Monika Pontikidou

SID: 1104220016
Supervisor: Dr. Venetia Argyropoulou

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

February 2024
Thessaloniki - Greece

Abstract

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation at the International Hellenic University.

The aim of the dissertation is to explore the application of the General Data Protection Regulation in electronic contracts, taking into account potential challenges arising in the digital landscape and providing suggestions for accomplishing data protection and digital privacy. Chapter I begins with a general overview of the GDPR, seeking to define key terms and concepts of the regulation. Chapter II introduces the concept of e-contracts, including a distinction of the different types of agreements formulated online, an analysis of the requirements of e-contract validity, as well as the issue of electronic signatures. The following part of the dissertation explores the interrelation of e-contracts and the GDPR and, more specifically, how data protection principles and the bases for lawful data processing, the two cornerstones of the Regulation, can be implemented in e-contracts to uphold the principles of transparency, accuracy and accountability.

Subsequently, an appraisal of relevant case law through recent landmark cases of the CJEU, provides valuable insights into the practical challenges faced by individuals and corporations alike regarding privacy and data security. Finally, this dissertation will seek to present some best practices for organizations to address privacy concerns in digital contracts, including a mention to recommended techniques and policies, the exercise of data subject rights and the implementation of privacy by design, with a view to respond to specific digital threats and ensure GDPR compliance.

Lastly, I would like to thank my supervisor, Dr. Venetia Argyropoulou, for her contribution in this dissertation.

Keywords: GDPR, e-contracts, personal data, privacy, data protection

Vasiliki Monika Pontikidou
February 2024

Contents

Introduction

The dawn of the 21st century heralded the world's definitive entry into the era of the so-called 'information society'. Unceasing technological advancements led to the globalization of markets and the birth of digital commerce, unveiling new opportunities for individuals and businesses around the world. Yet, as with all opportunities, this transition from conventional to digital commerce came with its own set of challenges. Decades later, as electronic contracting has evolved into a quotidian affair and new types of agreements are formulated online at the click of a button, the imperative of safeguarding consumer rights looms large.

In this vein, the issue of personal data protection has been met with new implications, as the ceaseless flow of data streams in digital transactions demands diligence and foresight. In todays 'data society', the GDPR is undeniably the most influential framework in the field of data privacy. Enacted in 2018, this landmark legislation aspired to harmonize data protection laws across Europe. It quickly proved profoundly successful and with a far-reaching effect that has allowed multinational companies to adopt uniform and effective data protection frameworks. However, considering how e-commerce has allowed businesses to process data on a global scale, the risks for data breaches and misuse have multiplied.

This dissertation seeks to explore precisely this intricate relationship between GDPR considerations and e-contracts, examining how the GDPR principles and requirements come into play from the early stages of e-contracting, up until the subsequent concerns of data storage, retention and security. Key themes such as consent mechanisms have proven to be controversial, leading to insightful judgments of the CJEU that are going to be analyzed, offering a guide to organizations on ensuring the validity and lawfulness of e-contracts from their very creation. Furthermore, through a comprehensive analysis of suggested practices, policies and technologies, this dissertation endeavors to provide practical recommendations to solidly implement data privacy safeguards in e-contracting environments.

Ultimately, in this era defined both by innovation and ambiguity, examining legal intricacies and technological nuances is imperative to balance the stakes of data

protection and privacy against this backdrop of an ever-evolving digital and legal landscape.

I. **Understanding the General Data Protection Regulation**

Personal data is any information that relates to an identified or identifiable living individual. They range from a person's name and age to their occupation, marital status, their photo, dietary restrictions, shopping habits and much more. A distinct category among them is sensitive personal data, which include genetic, biometric and health-related data, as well as data relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, their sex life and sexual orientation[1].

In 2016, with the development of technology and the internet holding an ever-present role in our lives, it became evident that personal data needed to be protected through a regulatory tool that would harmonize already existing national laws and set stricter and more effective terms. The General Data Protection Regulation was adopted in 2016 and became enforceable two years later and it can be considered the successor to the EU's 1995 Data Protection Regulation. Its aim is to regulate the collection, use and destruction of personal data and to uphold the right to privacy and the safeguarding of personal data, which are protected through national constitutions as well as Article 8 of the EU Charter of Fundamental Rights. To this end, Recital 2 of the GDPR states that "*The Regulation aims to achieve an "area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of economies within the internal market and to the well-being of natural persons*[2]*."*

The Regulation applies to the processing of personal data. Processing is defined in the Regulation as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (…), such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise*

[1] "What Personal Data Is Considered Sensitive?" European Commission. Accessed February 14, 2024. Available at https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en.

[2] Recital 2 of the GDPR

making available, alignment or combination, restriction, erasure or destruction;"[3]. More specifically, it applies to the processing of data of EU citizens, wherever they may be located.

The key provisions of the GDPR could be summarized as such: i) the requirement of valid consent for the collection, use and storage of personal data, ii) the rights of access, rectification and erasure, iii) the right to data portability, iv) the obligation to report data breaches to the relevant authorities, v) the requirement for implementing appropriate technical and organizational measures to ensure the security of personal data, and others.

Scope of the GDPR

The Regulation applies to the processing of personal data either by automated means or as part of a filing system *(material scope)*, when it relates to the offering of goods or services or the monitoring of the behavior of the data subjects, as long as they take place within the Union *(territorial scope)*. Additionally, the Regulation applies to a controller not established in the Union, but to a place where the law of a Member State is applied under public international law. [4]

Data controller and data processor

Article 4 (7) of the GDPR defines the data controller as *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data",* while Article 24 analyzes the principle of accountability and his responsibility to ensure that processing of personal data is done in accordance with the regulation[5].

On the other hand, the data processor is defined on Article 4 (8) as the *"natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".* The processor must meet the requirements set by Article

[3] Article 2 of the GDPR

[4] Kuner, Christopher, Lee A. Bygrave, Christopher A. Docksey, and Laura Drechsler. The EU general data protection regulation (GDPR): A commentary. Oxford: Oxford University Press, 2020, p. 12

[5] ibid, p. 26

28, which, among others, stipulates the terms that must govern the contract that needs to exist between the processor and the controller, for the former's actions to be regulated. Finally, it establishes the conditions that must be met for subcontracting another processor, as well as the responsibility of the initial processor[6].

Extraterritorial scope of the GDPR

The Directive's efficiency lies in its far-reaching effect, aided by the fact that it poses controls on personal data outside of Europe. This hinders powerful controllers like big companies from moving personal data to areas with less strict data protection rules. Therefore, even if the controller or processor is not established in the European Union, the GDPR still applies when the processing activities are related to offering goods or services to data subjects located in the EU[7] or when they are related to the monitoring of the behavior of such data subjects insofar as their behavior takes place within the Union[8]. For example, if an American company places cookies on the computers of people in the EU, the GDPR will apply.

Exceptions to the application of the GDPR

The GDPR's focus does not lie on individuals as much as companies and organizations. This is why it excludes from its scope *"purely personal or household activity"* (Article 2 par. 2 (c)). It also does not regulate public security and the prosecution of criminal offenses (Article 2 par. 2 (d)).

[6] Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." Information & Communications Technology Law 28, no. 1 (January 2, 2019): 65–98. Available at https://doi.org/10.1080/13600834.2019.1573501.

[7] Recital 23 of the GDPR

[8] Recital 24 of the GDPR

II. Aspects of e-contracts

Before this dissertation delves into exploring how the GDPR applies to e-contracts, it is crucial that the concept of electronic contracts themselves is defined and clarified.

Definition and types of e-contracts

Ever since civilized societies realized that the exchange of goods, on which everyday life was based, needed to be regulated, contracts -whether written or oral, formal or informal- became the pillar of the very first legal systems. Contracts can be defined as a legally binding agreement between two or more parties that creates legal obligations between them.

Centuries later, with the rise of electronic commerce, a new type of contract has emerged, which today might be even more prevalent than traditional contracts. An electronic contract can be defined as any kind of agreement created on a digital platform that is binding for its parties. It is an agreement created through digital interactions, without the parties actually meeting in person[9], while the digital environment where they are formed is often an *electronic market,* or a platform offering support for market transactions for the sale of goods and services[10]. E-contracts present many advantages compared to conventional ones, such as being more time-efficient, as they do not require lengthy face to face meetings and negotiations before reaching an agreement. Furthermore, they are mostly automated, which leads to fewer errors, while their digital nature diminishes unnecessary operational costs. However, e-contracts essentially perform the same function as

[9] Soni, Mitul, "Legal Issues and Jurisdiction Involved in E-Contracts: An Analysis" (August 2, 2023). Available at SSRN: https://ssrn.com/abstract=4528990

[10] Gisler, Michael & Stanoevska-Slabeva, Katarina & Greunz, Markus. "Legal Aspects of Electronic Contracts. Infrastructures for Dynamic Business-to-Business Service Outsourcing". (June 2000) Available at https://www.researchgate.net/publication/237307722_Legal_Aspects_of_Electronic_Contracts_Infrastructures_for_Dynamic_Business-to-Business_Service_Outsourcing_IDSO'00_Stockholm_5_-_6_June_2000

conventional ones and for that reason they need to comply to many of the same requirements in regards of validity, as will be analyzed.

Electronic contracts can be distinguished into the following types:

Shrink wrap: This type of agreement is widely used, especially by software companies. They are unsigned license agreements which bind the consumer by opening the software package or by using the software[11]. These actions then constitute an acceptance of the terms and conditions of the product by the consumer. Case law has ruled that shrink wrap agreements are indeed binding and enforceable, however the shrink-wrap terms should be available to the consumer at the time of the purchase. Otherwise, it is possible to back out of the contract upon examination of the terms after the purchase[12].

Click wrap: These agreements are extremely often used in practice, in cases where the consumer may not even be aware that they are entering into an agreement. In click wrap contracts, the consumer indicates their acceptance of the terms and conditions that the vendor displays, simply by clicking on a button, such as "I agree", "I accept" or even "OK". Usually, acceptance through clicking these choices is needed in order for the consumer to access the material of the website[13].

Browse wrap: In a browse wrap or web-wrap agreement, the user enters into a contract simply by using a website. Unlike click wrap agreements, there is no message upon entering the website containing the terms and conditions, with an option for the user to click "accept". In this type of agreement, the terms and conditions are retrievable through a link on the bottom of the website's homepage. Clearly, this poses problems regarding the enforceability of the contract when the user is not aware of the existence of such a link and the website has not properly notified the user. For example, in the case of *Pollstar v. Gigmania LTD*[14]-perhaps the first case dealing with browse wrap-, Pollstar was a website that provided users with

[11] Hayes, David L. "The Enforceability of Shrinkwrap License Agreements On-Line and Off-Line" Carnegie Mellon University (March 1997). Available at http://euro.ecom.cmu.edu/program/law/08-732/Transactions/ShrinkwrapFenwick.pdf.

[12] Gatt, Adam. "Electronic Commerce — Click-Wrap Agreements. The Enforceability of Click-Wrap Agreements." Computer Law & Security Review 18, no. 6 (November 2002): 404–10. Available at https://doi.org/10.1016/s0267-3649(02)01105-6.

[13] ibid

[14] Pollstar v. Gigmania LTD, Casemine. Accessed February 14, 2024. Available at https://www.casemine.com/judgement/us/5914ba16add7b0493478ef4e

information about concerts, that the user could download pursuant to the conditions of a license agreement. Pollstar alleged that Gigmania used information that had been downloaded from their website and posted it on its own website, thereby breaching the license agreement. The defendant Gigmania argued that the terms of the license agreement that the user was entering into are not clearly visible on the website. Indeed, a link to the terms did exist on Pollstar's webpage, but it was on gray print on gray background. The court found that even though the users were not given adequate notice of the license agreement, the agreement was still enforceable, because the user's conduct of proceeding to the webpage is considered as an implied acceptance of the existing terms and conditions.

Scroll wrap: In scroll wrap contracts, the agreement is displayed on the screen in a box that the user needs to scroll through before clicking the "I agree" or "I accept" button. This creates the presumption that the user has read all the terms and conditions that were made visible to them while scrolling. In *Newell Rubbermaid Inc. v. Storm*[15], it was ruled that the user had been given actual notice of the agreement, even if it only partially appeared on the scrollbox, because it was accompanied by the following disclaimer: *"To complete your Grant Agreement online, you must read and accept the terms outlined in the document posted above."* Even more so, the user cannot claim ignorance of the agreement when it was presented in its entirety in the scrollbox. In the case *RealNetworks, Inc. Privacy Litig*.[16] the court ruled that *"Because the arbitration agreement is not buried in fine print and because a user is given ample opportunity to understand the arbitration provision, the Court does not find that the arbitration agreement is procedurally unconscionable."*

Sign-in wrap: Finally, in sign-in wrap, the agreement is accepted by registering for or signing into a web-based service, such as logging into Facebook, where the terms and conditions are available during the sign-in process[17]. On many websites,

---

[15] Newell Rubbermaid Inc. v. Storm, Casetext. Accessed February 14, 2024. Available at https://casetext.com/case/newell-rubbermaid-inc-v-storm

[16] In re RealNetworks Inc. Privacy Litigation, Internet Library of Law and Court Decisions. Accessed February 14, 2024. Available at http://www.internetlibrary.com/pdf/In-re-RealNetworks-N.D.-Ill.-May-8-2000.pdf

[17] Kim, Nancy S. "Wrap Contracting and the Online Environment: Causes and Cures." Research Handbook on Electronic Commerce Law, California Western School of Law Research Paper No. 15-08 (August 24, 2015) Available at https://ssrn.com/abstract=2650132

upon signing in the user is greeted by a message such as *"By logging in you agree to (the website's) Terms of Service and Privacy Polic.*", where the words "Terms of Service" and "Privacy Policy" are hyperlinks to the respective documents[18]. In *Berkson v. Gogo[19],* the court found the sign-in wrap contract not binding because the terms of use were not "*readily and obviously available"* to the user, since *"the hyperlink to the 'terms of use' was not in large font, all caps, or in bold".*

Validity of e-contracts

In adherence to contract law, conventional contracts are formed through the exchange of an offer and its acceptance[20]. Other essential elements for the validity of the contract include the intent to establish legal relations, valuable consideration, legal capacity to enter into an agreement, genuine consent to the agreement and the legality of objects. In reality, e-contracts do not differ much from traditional contracts, especially since they have to meet many of the same requirements in order to be considered valid. An examination of these essential elements of standard contracts and how they are translated in the digital world, is necessary to examine the validity of e-contracts.

Offer and acceptance

In traditional transactions, an agreement between two parties becomes a legally binding contract when one party makes an offer to another party, which that party then accepts. The offer must be clear, complete and final, while the acceptance on the part of the offeree must correspond to all essential elements of the offer, making it unqualified and unconditional[21]. Additionally, the acceptance must be

[18] Russ, Brian, "All Wrapped Up and Nowhere to Gogo: Wrap Contracts Meet the Wrapture" (February 12, 2016). Available at https://ssrn.com/abstract=2731804

[19] Berkson v. Gogo LLC, Casetext. Accessed February 14, 2024. Available at https://casetext.com/case/berkson-v-gogo-llc-1

[20] Cooley , John W. "New Challenges for Consumers and Businesses in the Cyber-Frontier: E-Contracts, E-Torts, and E-Dispute Resolution." Loyola Consumer Law Review 13, no. 2 (September 2001): 102. Available at https://lawecommons.luc.edu/lclr/vol13/iss2/2

[21] Salzedo, Simon, Peter Brunner, and Michael Ottley. Briefcase on contract law. London: Cavendish, 2004.

communicated to the offeror either by words or conduct - in any case, silence cannot be construed as acceptance.

The above rules on offer and acceptance can also be applied in the digital landscape of electronic transactions. For example, a customer browsing a website offering goods or services is making an offer to the seller, which the seller then accepts when the order is completed, through an automated message of acknowledgement or confirmation.

In the digital world, the offeror can also be called *"the originator*", a term meaning the person who originates the electronic message through forms on their website and transmits it to the "*addressee"*[22]. These terms are used in the UNCITRAL Model Law on Electronic Commerce. Article 11 of the Model Law states that *"In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages."*[23] Article 2 (a) defines data messages as "*information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy"*. The addressee can then accept the offer by clicking the buttons "I agree", "I accept" or "Allow" on the originator's message. In some cases, the addressee must use a digital signature, which will be discussed later, to state acceptance of the offer.

While the UNCITRAL Model Law is not legally binding, it serves as a roadmap for the formation of electronic contracts and it is also considered the basis of the United Nations Convention on the Use of Electronic Communications in International Contracts (2005), which set more precise rules for electronic contracts in international trade. Namely, Article 12 of the Convention on the use of automated message systems for contract formation clearly states that a contract remains valid and enforceable

[22] Chahande, Jaimala. "An Analytical Study on E-Contract: Its Legal Validity and Jurisdiction." International Journal of Law Management & Humanities 3, no. 6 (2020). Available at https://doi.org/https://ijlmh.com/an-analytical-study-on-e-contract-its-legal-validity-and-jurisdiction/.

[23] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996

even if it is formed solely by the interaction of automated message systems, without being subjected to the review of a natural person.[24]

Another notable legal instrument is Directive 2000/31/EC, commonly known as the E-commerce Directive. Paragraph 1 of its Article 9 states that *"Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means"*[25], while Paragraph 2 establishes certain categories that can be exempted from the application of the previous paragraph. It is clear, therefore, that the Directive seeks to ensure for electronic contracts equal treatment to traditional contracts, reiterating the notion that the requirements for their validity are the same.

Consent

Voluntary and informed consent is necessary in contract law, as it signifies the meeting of the minds between the parties. In e-contracts, consent of the user needs to be established in order to determine the genuine intent of the parties. The originator should present the terms of the agreement in a clear and unambiguous manner to ensure that the user is fully informed. In traditional contracts, consent is normally given through the parties' signature. In the absence of paper agreements and physical signatures, some e-contracts may use digital signatures as a means of expressing consent. Explicit consent also manifests in affirmative actions of the user, such as clicking a checkbox.

The vastness and haziness of the digital landscape often set additional obstacles in the determination of an e-contract's validity. Often, there may not be clear requirements for the user's consent, which makes it difficult to confirm whether

[24] United Nations Convention on the Use of Electronic Communications in International Contracts

[25] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

it was truly voluntary and informed. This risk can be mitigated through *data retention*. The retention of the data messages that serve as the basis of the agreement between the parties, can serve as evidence of explicit consent, if they clearly express agreement or authorization. It can also ensure the messages' authenticity and integrity in cases where they are disputed. Different legal frameworks across many jurisdictions require data retention, for example regarding telecommunications laws that require the retention of data such as call records.

The issue of electronic signatures

Despite the many advantages of e-contracts, the digital environment hides some inherent risks. Because an electronic message is not imprinted on paper and bears no handwritten signature, it is indistinguishable from a copy. This increases the possibility of fraud, as it is difficult to establish the genuine intent of the message's addressee. Electronic signatures seek to mitigate this concern, by performing the same functions as handwritten signatures, but in an electronic setting.

The European Union's eIDAS Regulation (Regulation on electronic identification and trust services for electronic transactions in the internal market) establishes a legal framework for e-signatures, categorizing them into three types -simple, advanced and qualified- and recognizing them as equivalent to handwritten signatures. Article 25 states that *"1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. 2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.",* requiring their equal treatment to handwritten signatures.

First, *simple* e-signatures are defined as *"data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign"*[26]*.* Based on this definition, simply signing your name under an email can be considered an electronic signature. *Advanced* electronic signatures are

[26] Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Article 3 (10)

those that fulfill the requirements of Article 26, namely they are a) uniquely linked to and capable of identifying the signatory, b) created in a way that allows the signatory to retain control and c) linked to the document in a way that any subsequent change of the data is detectable. Typically, they can be provided using public-key infrastructure (PKI[27]), involving the use of certificates and cryptographic keys. Lastly, a *certified* electronic signature is an advanced e-signature, with the additional requirements that it is also a) created by a qualified signature creation device and b) is based on a qualified certificate for electronic signatures. A signature creation device is the hardware or software used to create e-signatures in a secure manner[28]. However, in order for it to be considered a *qualified signature creation device,* it needs to fulfill the requirements of Annex II of the Regulation, which are to ensure *"(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured; (b) the electronic signature creation data used for electronic signature creation can practically occur only once; (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology; (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others."*

The UNCITRAL Secretariat also mentions electronic signatures on its explanatory note on the United Nations Convention on the Use of Electronic Communications in International Contracts[29]. Apart from public-key infrastructure, there are techniques for authentication using a biometric device, where the user signs with a special pen either on a computer screen or on a digital pad[30].

---

[27] PKI is a technology used to ensure security of information through encryption. It commonly includes a public key, which anyone can use to encrypt a message, and a private or secret key, which only a specific person can use to decrypt it.

[28] Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Article 3 (22)

[29] United Nations Convention on the Use of Electronic Communications in International Contracts

[30] Heckeroth, J.. "Features of digitally captured signatures vs. pen and paper signatures: Similar or completely different?" Forensic Science International, Vol. 318 (2021). Available at https://www.sciencedirect.com/science/article/pii/S0379073820304497

Overall, the eIDAS Regulation aims to ensure the legal recognition and acceptance of e-signatures, while enhancing cross-border interoperability in electronic identification by establishing common rules for transactions across member states. The standards it sets for e-signatures are designed to provide a high level of security for consumers and businesses alike and address the challenges of fraud risks and lack of digital trust among consumers.

III. Implementation of GDPR in e-contracts

In order to assess how the GDPR can be applied to e-contracts, a presentation and analysis of the Regulation's core principles is essential. This chapter will review the GDPR's fundamental concepts, including data protection principles and the rights of data subjects, highlighting their direct relevance to e-contracting cases, as well as the bases for lawful processing recognized in the Regulation and their practical application in the context of e-contracts and finally, an assessment of relevant case law.

Data protection principles

The GDPR introduces a set of principles regarding the collection, processing and storage of personal data, that aim to protect the data subject and are summarized in Article 5.

Lawfulness, fairness and transparency

The first principle regarding personal data is that they need to be processed lawfully, fairly and in a transparent manner in relation to the data subject. In order for the processing to be considered *lawful*, it needs to comply with all applicable legal instruments[31]. Article 6 lists the core conditions, at least one of which needs to apply, for the processing to be lawful, which are going to be analysed more comprehensively later in this chapter. *Fair* processing suggests that data has not been acquired or otherwise processed through unfair means, by deception or without the data subject's knowledge. The *transparency* requirement is explained in Recital 39 of the GDPR. According to the Recital, the data subjects should be aware when their data is collected, used, consulted or otherwise processed, to what extent and for what specific purposes. Any relevant information should be easily accessible and in a clear and plain language. Data subjects should also be informed of risks, rules, safeguards, as well as their rights regarding the processing of their data.

[31] Kuner, Christopher, Lee A. Bygrave, Christopher A. Docksey, and Laura Drechsler. The EU general data protection regulation (GDPR): A commentary. Oxford: Oxford University Press, 2020, p. 314

Purpose limitation

The purpose limitation principle requires data to be *"collected for specified, explicit and legitimate purposes".* This means that the specific purposes need to be determined from the time of collection of the data. The principle of purpose limitation requires that data *is "not further processed in a manner that is incompatible with those purposes"*, which ensures that it is not repurposed for activities beyond the original intent that was disclosed to the data subject. The purposes also need to be legitimate, so that they do not limit the rights, freedoms and interests of the data subjects[32].

Data minimisation

Furthermore, the data that is processed must be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".* Recital 39 explains that the processing should be a last resort, only if the purposes cannot reasonably be fulfilled by other means and that it should not target information that is excessive and irrelevant to its purposes.

Accuracy

The GDPR explicitly requires that the controller ensures that the data is *"accurate and, where necessary, kept up to date".* Otherwise, it should be erased or rectified[33].

Storage limitation

This principle relates to the time period that data is stored. Specifically, it should be kept *"for no longer than is necessary for the purposes for which the personal data are processed".* The storage limitation principle makes an exception for the storage of data for longer periods, only *"for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".* Notably, Recital 39 suggests that, in order to ensure that data is stored only for the necessary period, time

[32] Kuner, Christopher, Lee A. Bygrave, Christopher A. Docksey, and Laura Drechsler. The EU general data protection regulation (GDPR): A commentary. Oxford: Oxford University Press, 2020, p. 315

[33] Ibid, p. 317

limits must be established by the controller for erasure or for a periodic review. Additionally, Article 25 of the GDPR on *data protection by default* recommends that the controller *"shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed",* which also applies to the period of storage of data that is not relevant to the specific purpose.

Integrity and confidentiality

Personal data needs to be processed in a manner that ensures their appropriate security, "*including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*. Chapter 4 of the Regulation, which relates to the obligations of the data controllers and processors, delves into more detail regarding the security of data, establishing requirements such as pseudonymization, encryption and the notification of data breaches to the supervisory authority.

Accountability

A cornerstone of the GDPR, this principle states that *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1".* This essentially means that organizations should implement suitable technical and organizational measures and further, should be capable of providing evidence of their actions and their effectiveness upon request[34]. This obligation entails compliance with all aforementioned data protection principles, as well as adequate documentation of the measures taken to achieve compliance. Such measures include the processes and procedures aimed at addressing data protection issues either at an early stage or when dealing with a data breach, such as adopting a 'data protection by design and by

[34] "Accountability" European Data Protection Supervisor. Accessed February 14, 2024. Available at https://www.edps.europa.eu/data-protection/our-work/subjects/accountability_en

default' approach, maintaining documentation of processing activities, appointing a Data Protection Officer or carrying out data protection impact assessments.

Lawful processing of personal data in the context of e-contracts

Considering the fact that any use of personal data is a potential limitation of the right to privacy and data protection, it becomes clear that data processing must be authorized in specific instances and for specific reasons. That is why the GDPR recognizes in its Article 6 six grounds for lawful processing. This constitutes an exhaustive list and at least one of these grounds needs to apply in any instance of processing. In order to explore how digital contracts can be designed with a view of complying with the right to privacy and protecting data subject rights, it is important to analyze the grounds for lawful processing and examine how they apply to e-contracts.

Consent of the data subject

Article 6 (1)(a) of the GDPR allows data processing if the data subject has given their consent for one or more specific purposes. It is important to note that lawful processing on the basis of the subject's consent is the only case where the processing can be stopped at the discretion of the data subject, by withdrawing that consent[35].

Article 4 (11) specifies that consent *"means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".* Individuals give their free consent when they not only have the option to refuse, but also to withdraw their consent, without external pressure or negative consequences[36]. Regarding the requirement for informed consent, organizations must implement a clear, intelligible and easily accessible way of requesting consent, providing the user with information about the purposes of the

[35] Kuner, Christopher, Lee A. Bygrave, Christopher A. Docksey, and Laura Drechsler. The EU general data protection regulation (GDPR): A commentary. Oxford: Oxford University Press, 2020, p. 339

[36] Article 7 (3) of the GDPR

processing, the identity of the controller, the categories of data, the recipients and the right to withdraw consent[37]. This is also connected to the condition of specific consent, in the sense that the data subjects must be aware of the specific purposes for which their data is being processed. If these purposes change or if the need for additional operations arises, the subject's consent is needed anew[38]. Lastly, for consent to be unambiguous, there needs to be a clear, affirmative and deliberate action of the user, manifesting their agreement to the processing of their personal data, such as a written or oral statement. In e-contracts, ticking a box constitutes valid consent[39], as opposed to silence, pre-ticked boxes or inactivity, which have been found to fall short of the requirements for unambiguous consent.

At this point, it is crucial to note some best practices that organizations should implement for obtaining consent in e-contracts. First, consent requests, whether in the form of a checkbox, a clickwrap agreement, a request for an electronic signature or even an explicit consent form, should use a language clear and easily understandable to the average person, and require affirmative action, such as clicking a button or ticking a checkbox, so that consent can be truly informed and unambiguous. To fulfil the GDPR's requirement for 'free' consent, controllers should not make it a condition for accessing goods or services, unless necessary for the performance of the contract.

Another practice that many organizations adopt to ensure compliance with data protection frameworks is *layered notices*. Layered notices present information about data processing activities into distinct layers of levels, through which the user can access more details progressively as needed, rather than in a single lengthy privacy notice[40]. Typically, they include a summary or overview of key information on data processing as a first layer. Users can then access additional layers containing more elaborate information, such as the types of information collected, the uses for this data, the legal basis for processing and any potential third parties with whom the data

[37] "Process personal data lawfully" European Data Protection Board. Accessed February 14, 2024. Available at https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en

[38] Ibid

[39] Recital 32 of the GDPR

[40] "What methods can we use to provide privacy information?" Information Commissioner's Office. Accessed February 14, 2024. Available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

may be shared[41]. Next, the notices present the user with their choices relating to the processing, which can be consent or opt-out and finally provide the organization's contact information that the user can use to access more information or address questions. The notices can also be tailored so that users receive the information most relevant to their specific interaction or transaction. For example, a website selling goods online can provide different notices during account creation, check-out or post-purchase communications with a buyer. Layered notices are useful because they present information in a transparent and user-friendly format, making it easier for users to navigate the notice and find the information they need, and thus enhancing trust towards the controllers.

Contractual obligation

According to Article 6 (1)(b) of the GDPR, data processing is justified in the context of a contractual relationship to the extent that it is necessary for the fulfilment of the contract. What is characterized as 'necessary' for the performance of a contract is an objective assessment that is made on a case-by-case basis, considering whether or not there are less intrusive means that could be used for the same purpose[42]. Contrary to the case of consent as a basis for processing, the data subject cannot unilaterally end processing of their data, except by terminating the contract, pursuant to applicable civil law. The above provision of the GDPR also refers to the precontractual stage as a possible ground for lawful processing.

In digital contracts specifically, processing of personal data may be necessary for the performance of a contract in a variety of cases. For example, in an online purchase, personal information such as the name, address, email, phone number and payment details are necessary to process an order and deliver the purchased goods to the customer. Similarly, in subscription services, such as streaming platforms or online

[41] "Ten steps to develop a multilayered privacy notice" Centre for Information Policy Leadership. Accessed February 14, 2024. Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/ten_steps_to_develop_a_multilayered_privacy_notice__white_paper_march_2007_.pdf

[42] Kuner, Christopher, Lee A. Bygrave, Christopher A. Docksey, and Laura Drechsler. The EU general data protection regulation (GDPR): A commentary. Oxford: Oxford University Press, 2020, p. 331

memberships, personal information is required to set up an account, provide personal access to subscribed content and manage billing of the service, or even at the 'pre-contractual' stage, when information about a potential customer's preferences is used to tailor the products or services offered. Lastly, sectors like travel or hospitality also require data processing for handling online bookings, reservations and ticket purchases. In such cases, controllers need to take all steps necessary to ensure that processing is limited only to what is absolutely necessary for the performance of the contract. The principles of data minimization and purpose limitation should be strictly adhered to, to enhance transparency and user trust. Limiting the volume and scope of the data collected allows for more efficient data management, since organizations do not have to analyse and maintain a big volume of unnecessary data, which in turn mitigates the risk of data breaches and data misuse.

Legal obligation

Article 6 (1)(c) of the GDPR introduce legal obligations as a lawful basis for processing personal data when necessary to comply with legal or regulatory requirements imposed on the data controller. The purpose of processing must be the fulfillment of that obligation. Legal provisions that merely authorize individuals to do something, instead of imposing a direct legal obligation, clearly do not constitute a legal obligation that justifies data processing[43]. In traditional contracts, such an obligation is, for example, the processing of data of employees by the employer for social insurance purposes.

Under the EU Data Retention Directive, telecommunications providers are required to retain data such as phone call records and internet usage logs, for specified periods, for the purpose of investigating serious crimes and ensuring national security. In digital contracts, too, there are often cases where data processing is necessary under a provision of various sources, such as EU law, national regulations or industry standards. For example, e-commerce platforms must collect and store customer data for tax reporting purposes. However, it is imperative to note that these legal requirements cannot override obligations derived from other legal instruments, such

[43] Ibid, p. 333

as the GDPR. In such cases, organizations need to strike a careful balance between these legal obligations and ensuring appropriate data protection and compliance with privacy laws.

Vital interests of the data subject or another natural person

Article 6 (1)(d) includes not only the vital interests of the data subject, but also of other natural persons, as a lawful basis for processing. According to Recital 46, a vital interest is one that is *"essential for the life"* of the individual, such as when *"processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters".* Such a case could include situations where the data subject's -or other natural person's- basic needs, such as health or housing, are threatened, requiring a situation of concrete and imminent danger[44].

As is clear, the definition of 'vital interests' can be ambiguous and difficult to apply in everyday transactions and, therefore, as the Recital states should be applied *"only where the processing cannot be manifestly based on another legal basis".* In the digital world, there are contracts that are concluded electronically that may involve tracking and sharing of personal data in cases of emergency. More specifically, processing location data, medical history or emergency contact information could be necessary to dispatch emergency services, administer medical treatment, or notify next of kin in life-threatening situations. An e-contract with a health monitoring system, such as a medical alert system, an app, a wearable fitness tracker or a smart health device, could serve as a basis for lawful processing. For example, widely used continuous glucose meters can share data with a parent, a partner or a doctor and issue medical alerts when they detect dangerous glucose levels. Similarly, e-contracts for security systems or surveillance cameras may require data processing to detect and respond to imminent threats and emergencies.

[44] Kuner, Christopher, Lee A. Bygrave, Christopher A. Docksey, and Laura Drechsler. The EU general data protection regulation (GDPR): A commentary. Oxford: Oxford University Press, 2020, p. 333

Performance of a task of public interest or exercise of official authority

Article 6 (1)(e) of the GDPR serves as the general basis for personal data processing for public sector purposes. Justification of processing based on this provision focuses on the controller and whether or not they have are carrying out a task in the public interest or in the exercise of official authority. According to Recital 46 of the GDPR, *"Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters".* These scenarios could be applied in e-contracts too. For instance, healthcare services or public health initiatives may implement electronic contracts that allow processing of personal data for disease surveillance or contact tracing during health emergencies. In these cases that deal with sensitive personal data, it is even more crucial that controllers ensure compliance with other GDPR principles, including data minimization, purpose limitation and data security.

Legitimate interests

Article 6 (1)(f) justifies data processing when it is *"necessary for the purposes of the legitimate interests pursued by the controller or by a third party".* In the context of e-contracts, a legitimate interest may be fraud prevention and security of the digital platform. These interests could require, for instance, user identity verification during account creation, monitoring of user activities to prevent unauthorized access to electronic networks[45], personal data processing to improve the quality of services or products through market research or customer surveys. As stated in Recital 47, marketing and advertising, as well as business operations and analytics, could potentially constitute legitimate interests for data processing in digital environments, for example through analysing said data to tailor advertising campaigns based on demographic data, interests or past purchases. However, as is explicitly stated it in Article 6 (1)(f), the interests of the controller cannot justify lawful processing in cases

[45] Recital 49 of the GDPR

where there are overriding interests or fundamental rights and freedoms of the data subject, which again underscores the necessity for balancing the two conflicting interests.

Assessment of relevant case law

Fashion ID

'Fashion ID'[46] is a landmark case of the CJEU that examines the concepts of determining the data controller, consent mechanisms and the responsibilities of joint controllers. The parties of the case were Fashion ID GmbH & Co. KG, an online clothing retailer, and Verbraucherzentrale NRW e.V, a German consumer protection association. The latter brought proceedings against Fashion ID for a breach of German data protection regulation, on the grounds that it had embedded Facebook's Like button as a plug-in in its website. Consequently, when a user entered the website, information about their IP address was forwarded to Facebook, irrespective of whether the user had clicked on said Like button or whether they had a Facebook account. Regarding these allegations, Fashion ID argued a lack of knowledge of Facebook's actions. Facebook Ireland on the other hand, acting as an intervening party, claimed that the user's IP address is converted into and saved as a generic IP address, which is not traceable back to the user.

The national court referred to the CJEU with a series of questions regarding data protection, based on the then applicable Directive 95/46 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data', which was replaced by the GDPR. Fashion ID claimed that, contrary to the findings of the German court, it was not a data controller, since it had no influence over the users' data that Facebook had access to, nor how Facebook used that data.

Directive 95/46 gave the exact same definition of 'data controller' as the GDPR, a definition whose aim in both legal instruments was to offer as broad a protection as

[46] Judgment of 29 July 2019, Fashion ID, C-40/17, EU:C:2019:629. Available at https://curia.europa.eu/juris/liste.jsf?num=C-40/17

possible to data subjects. In an earlier judgment (Jehovan todistajat[47]), the Court had found that "a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46". While a data controller can act alone or jointly with others, the joint responsibility of several actors for the same processing does not require each of them to have access to the personal data concerned, nor does it mean that the operators are all equally responsible. The CJEU determined Fashion ID to be a joint controller, considering that by embedding the social plug-in, it "exerts a decisive influence over the collection and transmission of the personal data of visitors", which would undoubtedly not have occurred without the plug-in. However, Fashion ID is not responsible for data processing operations by Facebook after the transmission of the data. Lastly, because of the joint controllership between the two, both actors must pursue legitimate interests in order for the processing to be legitimate, while Fashion ID is responsible for obtaining the lawful consent of its users, prior to the collection and transmission of their data.

Planet 49

In this pivotal case[48] on the issues of consent in e-contracts, the CJEU ruled that a pre-selected checkbox on a website does not meet the requirements for valid consent. Planet 49, an online gaming company, organized a promotional lottery on its website. Users who wished to participate had to provide their postcodes, names and addresses. They were then redirected to a webpage containing two explanatory messages, each containing a checkbox. Ticking the first checkbox would permit third party sponsors to contact the users, whereas the second checkbox, which was pre-ticked, enabled the setting of cookies which in turn allow advertising based on the user's interests. Checking at least the first checkbox was a prerequisite to participate in the lottery.

[47] Judgment of 10 July 2018, Jehovan todistajat, C 25/17, EU:C:2018:551. Available at https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-25/17

[48] Judgment of 1 October 2019, Planet 49, C-673/17, EU:C:2019:801. Available at https://curia.europa.eu/juris/liste.jsf?num=C-673/17

Unsurprisingly, on the issue of the validity of user consent for the storage of their information, the CJEU found that a pre-ticked checkbox which the user had to deselect to refuse their consent, could not be grounds of valid consent. The court stressed that the data subject's consent must be specific, for the processing of the particular data in question, and not relating to other processing activities. Besides, Article 4 (11) of the GDPR expressly defines 'consent' as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;", therefore requiring an active and unambiguous behavior of the data subject. Recital 32 of the Regulation precludes "silence, pre-ticked boxes or inactivity" from the notion of consent. This is of course justified, as in practice, it is not possible to determine whether the deselection of the checkbox by the user was meant to signify consent, or whether the user simple did not notice the checkbox and the information contained therein or was not aware that they could deselect it.

The second question forwarded to the CJEU related to the information that the service provider must share with the website users regarding the cookies placed on their servers. Because the cookies assign a specific number to each user who provides their personal data, making them easily identifiable, they clearly constitute data processing. Therefore, the user needs to be informed of the functioning of the cookies, their duration and whether or not third parties may have access to them. In the context of the GDPR, this obligation is more expressly regulated, since Article 13 (1) and (2) establish the information that the data controller must share with the data subjects[49]

[49] Wiedemann, Klaus. "The ECJ's Decision in 'Planet49' (Case C-673/17): A Cookie Monster or Much Ado about Nothing?" IIC - International Review of Intellectual Property and Competition Law 51, no. 4 (March 23, 2020): 543–53. Available at https://doi.org/10.1007/s40319-020-00927-w.

Google Spain

The Google Spain case[50] is especially significant in the realm of online privacy and data protection. It originated from a complaint of a Spanish national, Mr. Coseja Gonzalez against the publisher of a large daily newspaper, as well as against Google Spain and Google Inc., on the basis that, upon a Google search, internet users could find links to pages of the newspaper, which included an announcement with Mr. Costeja Gonzalez's name under a real-estate auction for the recovery of social security debts. The dispute revolved around the applicant's wish for the newspaper to remove or alter the pages and for the links to be removed from Google's search results, claiming that they contained inaccurate and potentially harmful information about him, thereby breaching his right to privacy and data protection, under Directive 95/46.

Google Spain and Google Inc. presented to the CJEU the argument that firstly, search engines cannot be considered as engaging in the processing of data displayed in search results lists, as search engines process all available internet information without distinguishing whether or not they are characterized as personal data or not. Secondly, even if this activity was deemed as data processing, the operators of the search engines are not the data controllers, as they lack awareness of the data at hand and do not exert control over it. The Court referred to its landmark *Lindqvist* case, which had already decided that uploading personal data on the Internet constitutes data processing. Furthermore, recalling that Article 2 (b) of the Directive -now Article 4 (2) of the GDPR- expressly refers to the collection, retrieval, organization, storage, disclosure and dissemination of data as activities of data processing, considering that the operator engages in precisely those activities, they must clearly be classified as *processing*, irrespective of the fact that the data had already been published on the newspaper's website. Moreover, because the operator is the one determining the *purposes and means* of the processing activity, they must consequently be regarded as the *controller* and they are responsible for ensuring the lawfulness of the processing activities. After all, if the information relating to the data subject's private life did not appear on the list of search results on the search engine, it would most likely not have been accessible to the wide public, making the subject less easily identifiable and not

[50] Judgment of 13 May 2014, Google Spain, C-131/12, EU:C:2014:317. Available at https://curia.europa.eu/juris/liste.jsf?num=C-131/12

resulting in such a significant impact on their right to privacy. In light of the above considerations, Google Spain and Google Inc. were obliged to remove from their search results the links to web pages published by third parties and containing personal information, even if the publication itself on those pages may be lawful. The decision also recognized to Mr. Costeja Gonzalez the *right to be forgotten*, or the right that sensitive information, published more than fifteen years ago, be no longer linked to his name.

The case had far-reaching implications regarding the right of erasure and the right to be forgotten, raising a debate over the balance between the right to privacy, freedom of expression and the public's right to access information. It also brought to light the practical challenges of enforcing the right to be forgotten in the digital age and ensuring the lawfulness of data processing by websites and search engines alike.

Wirtschaftsakademie Schleswig-Holstein

Wirtschaftsakademie Schleswig-Holstein GmbH v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)[51] was another case exploring the definition of data controller and the responsibility of a fan page operator regarding Internet users' data protection. Wirtschaftsakademie was a company specializing in the field of education, which hosted a fan page on Facebook. It brought proceedings against a regional data protection authority that required it to deactive the fan page over an alleged infringement of Directive 95/46. The basis of this infringement was the fan page's failure to notify visitors that there cookies would be placed by Facebook on their hard disk, which would allow Facebook to collect their personal data, in order to gather statistics for Wirtschaftsakademie and share targeted advertisements to users.

Cookies are used for *web tracking*, which aims to optimize website functions, by monitoring users' online activities and interactions. Under Directive 95/46, the collection of personal data for the above purpose cannot be carried out without prior notification and consent of the user. The debate which the CJEU was asked to decide on, revolved around Wirtschaftsakademie's argument that it had no relation to

[51] Judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388. Available at https://curia.europa.eu/juris/liste.jsf?num=C-210/16

Facebook's data processing operations and therefore could not be characterized as a data controller, since Facebook was the one determining the purposes and means of the data collection and processing.

In its judgment, the CJEU stressed that the Directive, as well as the GDPR today, seek to provide a high level of protection of the fundamental rights and freedoms of data subjects and that accepting a narrow definition of the concept of controller would limit that protection. Recalling its judgment in the *Google Spain* case, it highlighted the importance of broadening the definition of data controller. In this context, it stated that *"the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account",* thus determining various parameters of the processing and having a direct influence on it. Importantly, the processing could not even occur without the creation of the fan page by its administrator. The applicant's argument that it does not have access to the data does not preclude it from being regarded as a controller, even more so considering that Article 2 (d) of the Directive and Article 4 (7) of the GDPR, do not require the controller to exercise full control over all aspects of data processing. As the Advocate General mentions in his opinion, complete control has become considerably less frequent in practice[52]. The Advocate General also drew comparisons between the case in question and the Fashion ID case discussed earlier in this chapter, equating the fan page administrator and the operator of a website that embedded Facebook's *Like* button in the form of a social plug-in, enabling the collection of visitors' data.

[52] Opinion of Advocate General, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2017:796. Available at https://curia.europa.eu/juris/liste.jsf?num=C-210/16

IV. Mitigating GDPR concerns in e-contracts

The GDPR introduced a robust and comprehensive framework for data processing, with the data protection principles and the bases for lawful processing serving as the two pillars on which organizations must base their privacy policies. In the digital world specifically, new legal considerations have emerged, stressing the need for recognizing the challenges in GDPR compliance and implementing best practices in electronic contracts.

Data security threats in e-contracts

In order to build strong data protection systems in the digital landscape, it is imperative to understand the types of data breaches that threaten digital privacy. A data security threat is *"any action that could jeopardize the confidentiality, integrity or availability of data"*[53]*.* They can come various sources and are detrimental to data controllers and users alike.

A *cyberattack* is a malicious attempt to unlawfully enter computer systems and steal, modify or destroy data. *Malware* stands for malicious software and includes worms, viruses and spyware hidden in a trusted email attachment or program, that when opened gives the attackers access to the targeted environment, while a *ransomware* is a type of malware that targets organizations, threatening data security or blocking access to data until a ransom is paid. A serious and ever-present threat is *insider information* about data, computer systems and security practices, that individuals can take advantage of to harm the organization. On the other hand, *unintentional exposure* involves employees who unknowingly and unwillingly provide unauthorized access to data. Lastly, *phishing* is the practice of sending fraudulent emails from seemingly trustworthy sources, aiming to trick individuals into revealing vital information such as passwords and access codes.

[53] Gargiulo, Michael. "Council Post: Data Security Threats: What You Need to Know." Forbes, May 16, 2022. Accessed February 14, 2024. Available at https://www.forbes.com/sites/forbestechcouncil/2022/05/16/data-security-threats-what-you-need-to-know/.

Best practices for GDPR compliance

Considering the strict requirements set by the GDPR, it is evident that organizations must act proactively and effectively to ensure that e-contracts comply with the Regulation's principles. Lawful and transparent data processing requires comprehensive data mapping, or the creation of a detailed and organized inventory of all personal data that the organization collects and processes, including how and why the data is processed, where it is stored and to whom it is transferred. Second, clear and explicit consent mechanisms, pursuant to the requirements analyzed in this dissertation, must be in place, to ensure that users are capable of giving their informed, explicit and unambiguous consent.

Furthermore, e-contracts should be designed according to the principles of data minimization and purpose limitation, to avoid the risk of unlawful data processing. Organizations must also take all necessary measures to ensure the security of the data stored and prevent illegal access. Such measures include *encryption* techniques, which protect data by converting it into ciphertext[54], which can only by decrypted using the corresponding decryption key. *Access control mechanisms* can be used to regulate access to personal data, utilizing special permissions and strong authentication methods, such as multi-factor authentication, and granting access on a need-to-know basis. A valuable technique for safeguarding sensitive information and reducing the risk of unauthorized access is *data masking.* Data masking or data obfuscation is a process of changing data values, using character shuffling, word substitution and encryption, while retaining the same format, to create a fake but realistic new version of them. Afterwards the data cannot be deciphered or reverse-engineered, which makes data useless to a potential attacker, while still allowing access by authorized users[55]. Finally, controllers and processors should take all

[54] "*Cipher is an algorithm which is applied to plain text to get ciphertext. It is the unreadable output of an encryption algorithm"* from "What is 'ciphertext'". The Economic Times. Accessed February 14, 2024. Available at https://economictimes.indiatimes.com/definition/ciphertext

[55] "What is data masking". Imperva. Accessed February 14, 2024. Available at https://www.imperva.com/learn/data-security/data-masking/

necessary steps to ensure the security of personal data pursuant to Article 32 of the GDPR[56].

An effective tool for preventing and detecting data threats are *Data Loss Prevention (DLP) solutions.* DLP solutions use a combination of processes and technologies, such as firewalls, antivirus software, AI and machine learning, to protect personal data from malicious activity[57]. The three types of DLP are *network DLP*, which analyzes the organization's network activity, *endpoint DLP*, which checks network endpoints such as serves, computers and mobile devices, and *cloud DLP,* which protects data stored in the cloud. After establishing all necessary security measures, regular compliance audits are advisable, so that the compliance of e-contracting processes and data processing activities with GDPR requirements can be assessed and areas for improvement can be identified. To that end, organizations must maintain accurate and updated documentation of the compliance measures implemented in e-contracts, such as the privacy policies, data processing agreements and records of data subject consent.

Moving from prevention to incident response, organizations need to develop a comprehensive *data breach response plan*, to ensure that they can swiftly and efficiently respond to the potential damage of a digital data breach. This strategy should clearly outline the actions and responsibilities of the staff that forms the response team, such as IT, legal, compliance, communications and executive leadership. Additionally, it needs to include steps for assessing and documenting the incidents, in order to identify the affected data subjects, and further, establish a

---

[56] *"The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: 1. the pseudonymisation and encryption of personal data; 2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; 4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing"* Article 32 of the GDPR

[57] Boehm, Amber. "What is Data Loss Prevention (DLP)?" Crowdstrike, December 15, 2023. Accessed February 14, 2024. Available at https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/

strategy for data recovery, such as restoring data from backups, improving security measures and conducting post-incident reviews[58].

Lastly, organizations must enable data subjects to exercise their rights to access, rectify and update their personal data. Firstly, the *right of access,* established in Article 15 of the GDPR, allows the data subject to request from the controller confirmation on whether or not their personal data are being processed, information about the processing and a copy of their data[59]. The right of access grants data subjects control over their data as it allows them to *"be aware of, and verify, the lawfulness of the processing[60]".* Especially in electronic contracts where users may give their consent to processing without fully understanding the implications, it is important that they can be made aware of the extent and scope of the processing of their data.

Secondly, the *right to rectification* under Article 16 of the Regulation empowers data subjects to ensure the accuracy of their processed personal data, by requesting the correction or completion of inaccurate or incomplete data. In e-contracts, individuals can address the request to the controller by contacting them through the contact channels that are often provided in controllers' websites.

Thirdly, the *right of erasure* or *right to be forgotten,* recognized in Article 17 of the Regulation, allows the data subject to request the erasure of their data, *"where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation"[61].* Controllers are obliged to comply with this request, except where

[58] "Data breach preparation and response" Australian Government, Office of the Australian Information Commissioner. Accessed February 14, 2024. Available at https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/

[59] "Guidelines 01/2022 on data subject rights, Version 1.0 Adopted on 18 January 2022" European Data Protection Board. Available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

[60] Recital 63 of the GDPR

[61] Recital 65 of the GDPR

retention of the data is necessary for the reasons referred to in Article 17 (3)[62]. Clearly, in the digital world there are a number of new challenges regarding the right to be forgotten, as was highlighted in the Google Spain case. In the vast expanse of the Internet, making copies of publicly available data is increasingly easy, rendering it almost impossible to locate all personal data items about a person, to verify the person's right of erasure and to determine the authority and jurisdiction that can authorize the deletion of all copies[63]. In the context of e-contracts concluded in a corporate digital network, this risk is mitigated when access to them requires a strong authentication of all users, so that their electronic identity can be linked to natural persons, whereas in the public portion of the web, online identities cannot be reliable, allowing an infinite distribution and replication of data[64].

Implementing privacy by design in e-contracts

Article 25 of the GDPR encourages controllers to "both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". In the context of e-contracts, privacy by design ensures that privacy measures are integrated into the contractual framework, to proactively guarantee the maximum protection of privacy of users. Such appropriate 'technical and organisational measures' include pseudonymization and Data Protection Impact Assessments (DPIAs).

[62] Markham, Keith. A practical guide to the general data protection regulation (GDPR). Minehead, Somerset: Law Brief Publishing, Ltd., 2018, p. 43

[63] "The right to be forgotten - between expectations and practice" European Union Agency for Cybersecurity. Available at https://www.enisa.europa.eu/publications/the-right-to-be-forgotten

[64] ibid

Pseudonymization

It must be noted that absolute data protection and privacy is achieved through data anonymization. However, taking into account that the GDPR applies to data that relates to an identified or identifiable natural person, it is clear that the Regulation does not apply in anonymized data[65]. Therefore, where complete anonymization cannot be achieved, the process of *pseudonymization* can be applied. Pseudonymization is defined in Article 4 (5) as *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".* In this way, personal data can be attributed to a natural person by the use of additional information[66]. Pseudonymization employs the method of replacing an attribute with another, meaning that *"the identity of the subject is, but at the same time the ability to identify him/her"[67].* The identifiability aspect is important when the controller needs to collect more data from the same subject but without knowing their identity, as well as to keep information attributable to each data subject.

Data Protection Impact Assessments (DPIAs)

In cases of high-risk data processing, depending on the nature, scope, context and purposes of the processing, the GDPR provides in its Article 35 another measure for ensuring the safeguarding of personal data, the Data Protection Impact Assessments (DPIAs). Processing involving new technologies is explicitly mentioned in Paragraph 1 as a type of processing where the controller shall *"prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".* With this provision, the Regulation seeks to implement an assessment and identification of risks by the controller prior to processing.

[65] Recital 26 of the GDPR

[66] Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulation." Computer Law & Security Review 33, no. 2 (April 2017): 171–81. Available at https://doi.org/10.1016/j.clsr.2016.11.002.

[67] ibid

When preparing for a DPIA, the goals and scope of the assessment need to be determined first. If the organization has designated a Data Protection Officer, they also must be consulted[68]. In this preparatory phase, the actors involved in the processing need to be identified and any relevant sector-specific legal requirements need to be addressed[69]. Next, the DPIA needs to identify potential risks and attackers and their motives. According to this evaluation, the data processing activities are categorized according to their risk level into three protection standards: *normal*, for processing without potential for intense interference, *high,* for processing of Article 9's special categories of data, and *very high* for *"data requiring a high protection standard are processed and the person concerned depends on the decisions/services of the organization to an existential level and there are additional risks posed by insufficient data security or illegitimate changes of the purposes of processing, which the persons concerned cannot become aware of and/or correct by themselves"*[70]. After this evaluation stage, a plan for risk management is devised, which according to Article 35 (7) must contain the measures for risk mitigation, including safeguards, security measures and mechanisms for data protection. Finally, a report is published on the findings of the DPIA, which is then evaluated by an independent third party.[71]

As far as e-contracts are concerned, DPIAs are increasingly useful for websites with heavy traffic processing a significant volume of personal data. Taking into account that electronic systems are not fool-proof and sometimes depend on precarious technology, susceptible to threats from accidental data loss to cyber-attacks, DPIAs can be used to develop an effective strategy to anticipate and respond to risks. Recital 91 of the GDPR states that DPIAs are necessary in *"large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in*

[68]Article 35 (2) of the GDPR

[69] Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation." Privacy Technologies and Policy, 2016. Available at https://www.researchgate.net/publication/319276698_A_Process_for_Data_Protection_Impact_Assessment_under_the_European_General_Data_Protection_Regulation

[70] ibid

[71] ibid

accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights". Therefore, organizations that process the data of a mass number of users who enter into an electronic agreement at the click of a button, can greatly benefit from DPIAs to ensure GDPR compliance and safeguard both their interests, as well as the users'.

Conclusions

In summarizing the key insights acquired from this dissertation, it is clear that the GDPR is present in all stages of electronic contracting. From preliminary steps to ensure data security, to the formation of a valid contract based on transparent and informed consent mechanisms, GDPR requirements need to be followed to guarantee lawful and secure processing. Subsequently, during the performance of the e-contract, data minimization, purpose limitation, security and confidentiality are the keys to build trust between users and controllers and eliminate digital privacy threats.

Looking ahead, the landscape of e-contracts remains evolving and presents both opportunities and challenges. Technologies such as blockchain, artificial intelligence, machine learning have already been integrated in contracting processes to create the so-called 'smart contracts', posing more challenges for transparency, accuracy, security and compliance with regulatory frameworks. An emerging issue in this context is the one of accountability in cases where the human element is absent, considering that in such decentralized systems, decision-making may be governed by predefined algorithms that make it difficult to assign responsibility to individual actors. In such cases, accountability becomes intertwined with transparency, requiring the development of records of transactions and processes to trace decisions back to responsible parties and demanding an interdisciplinary approach to address technical, legal and ethical considerations. Furthermore, the Internet of Things (IoT) has created a vast network of interconnected devices, equipped with sensors and software to collect and act upon data. The challenge that raises privacy concerns is how these aspects of connectivity, interoperability and automation can guarantee compliance with GDPR requirements and ensure data privacy.

Regarding the Regulation itself, it remains interesting to see if and how other countries may adopt similar regulations and how the global effect of the GDPR may influence global data protection strategies in international organizations and companies. Additionally, the case law of the CJEU will continue to provide valuable insights into the practical implications of data processing in digital contracts. There have already been landmark judgements on cases of global companies, such as Facebook and Google, that had at their core the conflict between individuals' privacy,

corporate interests and democratic principles, such as the freedom of information and freedom of expression. It is certain that such cases of delicate balancing between conflicting rights will continue to gather global attention and create new precedents in digital contracting and data processing.

To conclude, the digital economy built upon e-contracts is entirely dependent on stakeholders navigating these changes to anticipate and respond to challenges, with a view to uphold privacy, transparency and accountability. Ultimately, it has become evident that the GDPR has set a new standard extending beyond the borders of the European Union and that compliance with its requirements is an ongoing process, demanding a deep integration of data protection principles into the architecture of electronic contracts.

Bibliography

LEGISLATION

"Guidelines 01/2022 on data subject rights, Version 1.0 Adopted on 18 January 2022" European Data Protection Board. Available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996

United Nations Convention on the Use of Electronic Communications in International Contracts

United Nations Convention on the Use of Electronic Communications in International Contracts

CASES

Berkson v. Gogo LLC, Casetext. Accessed February 14, 2024. Available at https://casetext.com/case/berkson-v-gogo-llc-1

In re RealNetworks Inc. Privacy Litigation, Internet Library of Law and Court Decisions. Accessed February 14, 2024. Available at http://www.internetlibrary.com/pdf/In-re-RealNetworks-N.D.-Ill.-May-8-2000.pdf

Judgment of 1 October 2019, Planet 49, C-673/17, EU:C:2019:801. Available at https://curia.europa.eu/juris/liste.jsf?num=C-673/17

Judgment of 10 July 2018, Jehovan todistajat, C 25/17, EU:C:2018:551. Available at https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-25/17

Judgment of 13 May 2014, Google Spain, C-131/12, EU:C:2014:317. Available at https://curia.europa.eu/juris/liste.jsf?num=C-131/12

Judgment of 29 July 2019, Fashion ID, C-40/17, EU:C:2019:629. Available at https://curia.europa.eu/juris/liste.jsf?num=C-40/17

Judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388. Available at https://curia.europa.eu/juris/liste.jsf?num=C-210/16

Newell Rubbermaid Inc. v. Storm, Casetext. Accessed February 14, 2024. Available at https://casetext.com/case/newell-rubbermaid-inc-v-storm

Opinion of Advocate General, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2017:796. Available at https://curia.europa.eu/juris/liste.jsf?num=C-210/16

Pollstar v. Gigmania LTD, Casemine. Accessed February 14, 2024. Available at https://www.casemine.com/judgement/us/5914ba16add7b0493478ef4e

BOOKS

Kuner, Christopher, Lee A. Bygrave, Christopher A. Docksey, and Laura Drechsler. The EU general data protection regulation (GDPR): A commentary. Oxford: Oxford University Press, 2020

Markham, Keith. A practical guide to the general data protection regulation (GDPR). Minehead, Somerset: Law Brief Publishing, Ltd., 2018

Salzedo, Simon, Peter Brunner, and Michael Ottley. Briefcase on contract law. London: Cavendish, 2004.

ARTICLES AND ONLINE JOURNALS

Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. “A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation.” Privacy Technologies and Policy, 2016. Available at

https://www.researchgate.net/publication/319276698_A_Process_for_Data_Protection_Impact_Assessment_under_the_European_General_Data_Protection_Regulation

Bolognini, Luca, and Camilla Bistolfi. “Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulation.” Computer Law & Security Review 33, no. 2 (April 2017): 171–81. Available at https://doi.org/10.1016/j.clsr.2016.11.002.

Chahande, Jaimala. “An Analytical Study on E-Contract: Its Legal Validity and Jurisdiction.” International Journal of Law Management & Humanities 3, no. 6 (2020). Available at https://doi.org/https://ijlmh.com/an-analytical-study-on-e-contract-its-legal-validity-and-jurisdiction/

Cooley , John W. “New Challenges for Consumers and Businesses in the Cyber-Frontier: E-Contracts, E-Torts, and E-Dispute Resolution.” Loyola Consumer Law Review 13, no. 2 (September 2001): 102. Available at https://lawecommons.luc.edu/lclr/vol13/iss2/2

Gatt, Adam. “Electronic Commerce — Click-Wrap Agreements. The Enforceability of Click-Wrap Agreements.” Computer Law & Security Review 18, no. 6 (November 2002): 404–10. Available at https://doi.org/10.1016/s0267-3649(02)01105-6.

Gisler, Michael & Stanoevska-Slabeva, Katarina & Greunz, Markus. “Legal Aspects of Electronic Contracts. Infrastructures for Dynamic Business-to-Business Service Outsourcing”. (June 2000) Available at https://www.researchgate.net/publication/237307722_Legal_Aspects_of_Electronic_Contracts_Infrastructures_for_Dynamic_Business-to-Business_Service_Outsourcing_IDSO'00_Stockholm_5_-_6_June_2000

Hayes, David L. “The Enforceability of Shrinkwrap License Agreements On-Line and Off-Line” Carnegie Mellon University (March 1997). Available at http://euro.ecom.cmu.edu/program/law/08-732/Transactions/ShrinkwrapFenwick.pdf

Heckeroth, J.. “Features of digitally captured signatures vs. pen and paper signatures: Similar or completely different?” Forensic Science International, Vol. 318 (2021). Available at https://www.sciencedirect.com/science/article/pii/S0379073820304497

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. “The European Union General Data Protection Regulation: What It Is and What It Means.” Information & Communications Technology Law 28, no. 1 (January 2, 2019): 65–98. Available at https://doi.org/10.1080/13600834.2019.1573501.

Kim, Nancy S. “Wrap Contracting and the Online Environment: Causes and Cures.” Research Handbook on Electronic Commerce Law, California Western School of Law Research Paper No. 15-08 (August 24, 2015) Available at https://ssrn.com/abstract=2650132

Russ, Brian, “All Wrapped Up and Nowhere to Gogo: Wrap Contracts Meet the Wrapture” (February 12, 2016). Available at https://ssrn.com/abstract=2731804

Soni, Mitul, “Legal Issues and Jurisdiction Involved in E-Contracts: An Analysis” (August 2, 2023). Available at SSRN: https://ssrn.com/abstract=4528990

“Ten steps to develop a multilayered privacy notice” Centre for Information Policy Leadership. Accessed February 14, 2024. Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/ten_steps_to_develop_a_multilayered_privacy_notice__white_paper_march_2007_.pdf

Wiedemann, Klaus. “The ECJ’s Decision in ‘Planet49’ (Case C-673/17): A Cookie Monster or Much Ado about Nothing?” IIC - International Review of Intellectual Property and Competition Law 51, no. 4 (March 23, 2020): 543–53. Available at https://doi.org/10.1007/s40319-020-00927-w.

WEBSITES

“Accountability” European Data Protection Supervisor. Accessed February 14, 2024. Available at https://www.edps.europa.eu/data-protection/our-work/subjects/accountability_en

Boehm, Amber. “What is Data Loss Prevention (DLP)?” Crowdstrike, December 15, 2023. Accessed February 14, 2024. Available at https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/

“Data breach preparation and response” Australian Government, Office of the Australian Information Commissioner. Accessed February 14, 2024. Available at https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/

Gargiulo, Michael. “Council Post: Data Security Threats: What You Need to Know.” Forbes, May 16, 2022. Accessed February 14, 2024. Available at https://www.forbes.com/sites/forbestechcouncil/2022/05/16/data-security-threats-what-you-need-to-know/.

“Process personal data lawfully” European Data Protection Board. Accessed February 14, 2024. Available at https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en

“The right to be forgotten - between expectations and practice” European Union Agency for Cybersecurity. Available at https://www.enisa.europa.eu/publications/the-right-to-be-forgotten

“What is ‘ciphertext’”. The Economic Times. Accessed February 14, 2024. Available at https://economictimes.indiatimes.com/definition/ciphertext

“What is data masking”. Imperva. Accessed February 14, 2024. Available at https://www.imperva.com/learn/data-security/data-masking/

“What methods can we use to provide privacy information?” Information Commissioner’s Office. Accessed February 14, 2024. Available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

“What Personal Data Is Considered Sensitive?” European Commission. Accessed February 14, 2024. Available at https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en.