GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

OLIVIA

Handbook on Personal Data Protection for SMEs

Croatian Personal Data Protection Agency
Agencija za zaštitu osobnih podataka

GPDP GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

foi

UNIVERSITÀ DEGLI STUDI FIRENZE

VUB VRIJE UNIVERSITEIT BRUSSEL

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

ARC II – Handbook on Personal Data Protection for SMEs

Co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union and European Commission. Neither the European Union nor the European Commission can be held responsible for them.

The ARC II project has been co-funded by the European Union's citizens, equality, rights, and values Programme under **Grant Agreement No. 101072630**.

AUTHORSHIP

This study was led by ARC II team at the University of Florence (Erik Longo and Federica Camisa); for the AZOP participated Anamarija Mladinić; for the Italian Garante per la Protezione dei Dati Personali participated Luciano Versace and Annalisa Marsano; for the Vrije Universiteit Brussel participated Cong Yao and Ashwinee Kumar.

LINGUISTIC VERSION

Original: EN

The manuscript was completed in October 2024.

DISCLAIMER AND COPYRIGHT

This document is prepared for the project "GDPR Awareness Raising Campaign for SMEs" Arc II.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

TABLE OF CONTENT

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

EXECUTIVE SUMMARY

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, also known as "General Data Protection Regulation" or GDPR, represents a comprehensive legal framework that has significant implications not only for individuals and entities within the EU but also for organizations outside the EU that engage in business with EU member states. The purpose of GDPR is "the protection of natural persons with regard to the processing of personal data and on the free movement of such data" (Article 1). The GDPR has been in place since May 2018, replacing existing data protection laws in all EU countries.

Implementing a single, horizontal framework law, such as the GDPR, offers significant advantages for businesses by streamlining compliance requirements, promoting accountability in managing personal data, and ensuring uniformity in data protection standards across the European Union. Despite the GDPR's status as a directly applicable regulation within the EU legal order, this Regulation allows for certain flexibilities, granting Member States the authority to enact supplementary legislation that addresses specific national concerns. This discretion enables Member States to establish additional standards in areas such as the processing of health data, criminal convictions, the digital age of consent, and the circumstances under which an individual's data protection rights may be restricted.

Accordingly, all Croatian and Italian businesses and organizations must be aware that they must comply with the data protection standards and obligations set out in the GDPR, the Croatian Act, and the Italian Personal Data Protection Code (accordingly).

The General Data Protection Regulation (GDPR) necessitates substantial modifications across various operational sectors for most organizations. Regrettably, many small- and medium-sized enterprises (SMEs) lack the resources and expertise to navigate these changes independently.

Thanks to the expertise of the Italian and Croatian Data Protection Authorities, also acquired through the projects ARC and SMEData, this Handbook has been designed to assist the small and medium enterprise (SME) sector in becoming more compliant with the GDPR. ARC II has been specifically designed to help SMEs that may lack expertise and legal resources develop autonomously a path to comply fully with the GDPR. Specific requirements under personal data legislation are sometimes considered burdensome, particularly with regard to standard business activities carried out by SMEs. Affording appropriate protection for personal data can become a significant expense for an enterprise. On the other hand, data protection can be a crucial asset for any firm, enhancing its effectiveness and increasing consumers' and users' trust.

Even after more than six years of its application, compliance with the GDPR remains challenging for SMEs. Therefore, there is a strong need for the development of practical guidance and digital tools that can also be replicated in other Member States, adapted to SMEs needs to facilitate the implementation of GDPR obligations.

Thus, this Handbook is meant to be a simplified guide for SMEs to develop governance and organization that fully respects data protection in accordance with European and National law. It contains educational materials, FAQs, best practices, and experiences of the Italian and Croatian SMEs and DPAs.

Doing business usually entails processing personal data, i.e., information related to identified or identifiable entities (e.g., employees, customers, suppliers). Therefore, the GDPR applies to you. Consequently, it is essential to remember that:

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

- Customers' and employees' data are "personal data".
- Simply storing personal data electronically or in hardcopy constitutes "processing" of personal data.

Given the "legitimate purposes" to be achieved, such data must be relevant and not excessive; additionally, the data must be accurate and updated. Processing operations (such as collecting, communicating, or disseminating personal data) may also be carried out by the data processor (where appointed) and the persons in charge of the processing.

The content of this Handbook does not necessarily represent the official views of the European Union. The legal framework and information presented within reflect the state of the law as of 30 August 2024. The ARC II Consortium has made every effort to ensure the accuracy and reliability of the information contained in this Handbook. Nevertheless, the ARC II consortium disclaims any liability for errors or omissions in the content provided. This Handbook is intended for informational purposes only and should not be construed as substituting professional or legal advice.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

1. Introduction

This handbook is one of the final outcomes of the Awareness Raising Campaign for SMEs (ARC II) project, which was co-funded by the European Union under Grant Agreement No. 101072630 under the call CERV-2021-DATA.

The ARC II project was implemented by a partnership of the Croatian National Authority for Data Protection (AGENCIJA ZA ZASTITU OSOBNIH PODATAKA - AZOP) (coordinator), the Italian National Authority for Data Protection (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI - GPDP), the University of Florence (UNIFI), the Vrije Universiteit Brussel (VUB), and the SVEUCILISTE U ZAGREBU, FAKULTET ORGANIZACIJE I INFORMATIKE between September 2022 and August 2024.

ARC II consortium included academics with extensive theoretical backgrounds in privacy and data protection – Paul Quinn (VUB) and Erik Longo (UNIFI) – academics with knowledge on building teaching materials for the large public in the field of data protection; Anamarija Mladinić as representative of the Croatian Data Protection Authority, and Luciano Versace as representative for ARC II project for the Italian Data Protection Authority, who have been actively engaged in awareness raising activities for SMEs during the last ten years.

The project's main goal was to promote compliance with the General Data Protection Regulation (EU) 2016/679, here-and-after GDPR, by stimulating awareness on EU and National rules on personal data protection regarding Small and Medium-sized Enterprises (SMEs).

This Handbook is designed explicitly for GDPR compliance, complementing the work done during the ARC II project to help SMEs independently build a data protection-compliant organization. This work supplements the main deliverable of the ARC II project, the OLIVIA web tool (see below). OLIVIA - which is the main goal accomplished by the Consortium within the ARC II project - provides a fully-fledged range of material, from interactive videos to teaching tools for compliance with European and National Regulations, as well as to raise awareness on personal data protection among the general public. All these tools are meant to facilitate compliance with the obligations arising out of the legislation in force and to highlight the simplification measures that are currently available.

Overall, the expected direct result of the ARC II project is increased knowledge and understanding among SMEs of their obligations arising from the GDPR and Italian and Croatian data protection legal framework. The project has increased GDPR compliance with digital tools developed in open-source code. Therefore, all the data protection authorities (DPAs) could adapt it to their national legislation and language. In this way, SMEs across the EU will benefit from the project results of the ARC II project.

ARC II has conceived this Handbook as a tool to intensify the awareness of the GDPR for SMEs. Making SMEs aware of the GDPR is not a simple task, and a Handbook cannot solve it. The ARC II approach has required many tools and a long-term strategy with efforts from public authorities, business associations, businesses, and society. Nevertheless, this Handbook represents an important stepping-stone that explains some of the main features of the GDPR (e.g., the principles, the roles, the risk-based approach, and the legal provisions embedding it) in more straightforward language. It also provides case studies, FAQs, and practical examples to structure the awareness of SMEs.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

In recognition of these challenges, this Handbook is specifically designed to raise awareness all over Europe and assist SMEs in achieving compliance with the GDPR. It is intended for SME owners and their representatives responsible for managing data protection matters, including internal and external Data Protection Officers (DPOs). The handbook may also be useful for SME associations.

We are aware that SMEs are not all the same. However, many face structural barriers (e.g., lack of human and financial resources) to attaining compliance with the GDPR, for which personal data processing is a collateral activity.

This Handbook follows a **structure** that tries to merge academic and practical points of view. It begins by offering essential definitions of key data protection concepts, emphasizing those most relevant to SMEs. Following this, the Handbook delineates the scope of data protection law within the European Union, focusing specifically on its applicability to SMEs. From the third section, the Handbook elucidates the fundamental concepts of EU data protection law, interpreting the relevant provisions of the GDPR that encapsulate these concepts, with particular attention given to the rules governing data protection impact assessments. The last section refers to the appropriate section of the OLIVIA tool. Each section includes practical examples, suggestions, and recommendations for further reading. The content of this Handbook is predominantly based on guidance documents provided by the two European data protection authorities partnering with the ARC II project. This Handbook draws upon a variety of existing handbooks and manuals published by Data Protection Authorities (DPAs) and European Union projects, many of which are specifically designed to guide GDPR compliance, as well as EDPB material. Some of these resources are particularly focused on SMEs.

As the scope of this handbook is limited to some of the topics of particular interest to SMEs, it is important to be able to navigate other available resources in the Olivia portal that are aimed at facilitating GDPR compliance.

Regarding the specific **method** used in this Handbook, it is necessary to remember that the topics mentioned above were of particular concern for SMEs during the numerous online and in-person meetings conducted during the project and, therefore, form the exclusive focus of this handbook. More specifically, the Consortium has conducted ten online interactive workshops and ten onsite workshops in Croatia and Italy, five interactive online train of trainers sessions in Croatia and five in Italy, organizing two international conferences, one in Rome and one in Zagreb, organizing two validation workshops, one in Zagreb and one in Florence.

The meetings, workshops, and conferences have been crucial to listing the topics of particular concern for SMEs, forming the exclusive focus of this Handbook. Based on the suggestions the different stakeholders have provided, the Handbook:

- Introduces to the GDPR and particularly to risk-based provisions.
- It includes examples and provides references to templates, guidance, and best practices developed by the Consortium's DPAs.
- Suggests how SMEs can achieve compliance with the GDPR and how to transform this into a competitive advantage.
- It targets a wide range of firms, regardless of their business sectors, with a specific interest in Croatian and Italian SMEs.
- Help create public awareness regarding the GDPR and the rights that it affirms.

The handbook is not intended as a silver bullet for solving all the challenges the GDPR poses to SMEs. Still, describing how the rules apply can improve the implementation and application of the GDPR.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

A. OLIVIA

The web tool Olivia is one of the most important results of the ARC II project. Its main objective is to support Croatian and Italian SMEs in implementing data protection legislation and principles in their day-to-day business activities.

Olivia is a virtual teacher and assistant at the same time. Olivia contains a small online academy that offers you a series of learning modules to improve your knowledge in the field of personal data protection and also serves as a practical tool to help you create internal documents to prove your compliance and reliability. Web tools in Olivia provide templates for GDPR documentation and clear and concise instructions on aligning their data processing activities with the Croatian and Italian data protection legal frameworks.

Go online and register (if you need help, please use the Manual):

- https://olivia-gdpr-arc.eu/
- https://olivia-gdpr-arc.eu/hr
- https://olivia-gdpr-arc.eu/italian/it

About the contents, Olivia includes 15 training courses on the most important issues of data protection legislation (from the basics of GDPR to the principles and legal bases of data processing, up to cookies' requirements or video surveillance systems in the workplace), each of which consists of a theoretical and practical module. Each of such courses includes not only educational materials, educational videos, knowledge tests, webinars, and presentations but also templates for drafting its own data protection compliance documentation. The theoretical part of the courses is made up of short lessons and a short webinar or educational video. After going through the theoretical part, there will be the opportunity to do the knowledge test. If there are more than 80% correct answers, Olivia will generate a certificate of successful completion of the theoretical module. Moreover, Olivia shares several webinars on different data protection matters and the relevant presentations used during such webinars. All webinars are permanent and free of charge, so users can view them anytime.

Additionally, the web tool allows companies to check their compliance status with data protection legislation by processing answers to the questionnaires provided.

The SMEs will then be able to deepen their knowledge of the topics addressed in this Handbook and train their data protection skills by using Olivia, too.

D. National Acts Implementing the GDPR

1. The Republic of Croatia

The General Data Protection Regulation (EU) 2016/679 ('GDPR') applies uniformly since 25th May 2018 in the European Economic Area (EEA), which encompasses the territory of the Member States of the European Union (EU) as well as Iceland, Liechtenstein and Norway. On the same date, in the Republic of Croatia entered into force Act on the Implementation of the GDPR, Official Gazette 42/2018, which ensures the implementation of the GDPR and sets out additional rules on the processing of personal data in specific circumstances.

Act on the Implementation of the GDPR ensures the application of the GDPR in Croatia and introduces additional provisions (Chapter IV of the Act) concerning the processing of personal data in specific scenarios, including:

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

- processing of children's personal data in relation to information society services;
- processing of genetic data;
- processing of biometric data;
- processing of personal data related to video surveillance;
- processing of personal for statistical purposes.

One important element to consider is related to Article 8(1) of the General Data Protection Regulation. It provides that the processing of personal data of a child in relation to the offering of information society services directly to the child is lawful if the child is at least 16 years old. If the child is under 16, such processing is only lawful if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. It is also established that Member States may provide for a lower age limit for this purpose, provided that such age limit is not lower than 13 years.

Article 19 of the Act on the Implementation of the GDPR stipulates that, with regard to offering information society services directly to a child, the processing of a child's personal data is lawful if the child is at least 16 years old.

Article 20 of the Act on the Implementation of the GDPR prohibits the processing of genetic data to assess the risk of disease and other health aspects of the data subject in the context of actions related to the conclusion or performance of life insurance contracts and contracts with survival clauses. The provision of paragraph 1 of this article applies to data subjects who conclude life insurance contracts and contracts with survival clauses in the Republic of Croatia if the processing is carried out by a data controller established in the Republic of Croatia or providing services in the Republic of Croatia. Consent cannot override this prohibition. In accordance with Article 21 of the aforementioned Act, the processing of biometric data in public authorities can only be carried out if it is provided for by law and is necessary for the protection of individuals, property, classified information, or business secrets, taking into account that the interests of the data subjects conflicting with the processing of biometric data under this article do not prevail.

According to Article 22 of the Act, the processing of biometric data in the private sector can only be carried out if it is prescribed by law or is necessary for the protection of individuals, property, classified information, business secrets, or for the individual and secure identification of service users, taking into account that the interests of the data subjects conflicting with the processing of biometric data under this article do not prevail. The legal basis for processing biometric data of data subjects for secure identification of service users is the explicit consent of such data subjects given in accordance with the provisions of the General Data Protection Regulation.

The processing of employees' biometric data for the purpose of recording working hours and for entry and exit from official premises is permitted if provided for by law or if such processing is carried out as an alternative to another solution for recording working hours or entry and exit from official premises, provided that the employee has given explicit consent for such processing of biometric data in accordance with the provisions of the General Data Protection Regulation (Article 23 of the Law).

The processing of personal data through video surveillance within the meaning of this Act relates to the collection and further processing of personal data that involves the creation of a recording that constitutes or is intended to be part of a storage system. **The processing of personal data through video surveillance can only be carried out for a necessary purpose and justified for the protection of individuals and property, taking into account that the interests of the data subjects conflicting with the processing of data through video surveillance do not prevail.** The law explicitly

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

regulates video surveillance of work premises, video surveillance of residential or mixed residential-business buildings, and video surveillance of public areas (Articles 25-32 of the Law).

It is important to emphasize that monitoring public areas through video surveillance is allowed only to public authorities, legal entities with public powers, and legal entities performing a public service, only if prescribed by law, if necessary for the performance of tasks and duties of public authorities, or for the protection of life and health of people and property.

More about video surveillance in Croatia you can find at Olivia-video surveillance modules.

While most data protection provisions aimed at the data protection of individuals in Croatia are found in the GDPR and the Act on the Implementation of the GDPR, there are many other laws and bylaws that prescribe specific rules for the processing of individuals' personal data (i.e. Labour Law, Credit Institution Act, Act on prevention of money laundering and funding on terrorism, Electronic Communications Act, Accounting Act, Consumer Protection Law, Family Act, Rulebook on the e-visitor system etc.).

It is very important for SMEs to know the legal framework of the industry in which they operate (e.g., financial, tourism, education, health, media, etc.) because, very often, a lawful basis for the processing of personal data and retention periods are prescribed by law.

With particular reference to Croatia, the Croatian Data Protection Authority ("AZOP"), in order to facilitate the correct implementation of the provisions of the GDPR, issued FAQs (Frequently Asked Questions) for SMEs on Lawful bases for processing of personal data, Records of processing activities, Informing individuals about processing of their personal data, Implementation of appropriate organizational and technical measures, Transfers of personal data to third countries, Processing of personal data for the direct marketing purposes and on duties and appointment of data protection officer.

2. The Republic of Italy

Italy implemented the GDPR by amending the Italian Personal Data Protection Code (legislative decree no. 196/2003, as supplemented by legislative decree no. 101/2018, the "Code"). The Italian Data Protection Authority ("Garante") supervises the GDPR and the Code.

The Garante has enacted a general guide on applying the GDPR (only available in Italian here), which provides high-level guidance on how to use it. The Garante has also published a number of Guidelines (only available in Italian here) and frequently asked questions ("FAQs") (only available in Italian here) on different topics related to the application of the GDPR (e.g., undesired marketing calls, video surveillance, etc.), which can be found in the institutional website.

Legislative Decree no. 101 of 10 August 2018 ("the Decree") amended the Code to coordinate the GDPR's provisions with Italian laws.

The Code provides for some peculiarities compared to the GDPR, in particular:

- **Children consent**: Article 2-quinquies of the Code provides that children who have reached the age of 14 can validly express their consent to data

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

processing concerning the offer of information society services. Where the child is under the age of 14 years, such consent must be provided by their responsible parent (see also section on special categories of personal data).

- **Rights concerning deceased persons**: according to Recitals 27 of the GDPR, Member States may provide for rules regarding the processing of personal data of deceased persons (to whom the GDPR does not apply). Article 2-*terdecies* of the Code prescribes that the rights referred to in Articles 15 to 22 of the GDPR concerning the personal data of deceased persons may be exercised by any entity having a vested interest or acting to protect the data subject as the latter's agent, or else on household-related grounds deserving protection. Exercise of these rights shall not be allowed where so provided for in a law or if the data subject has banned such exercise expressly by means of a written statement submitted or communicated to the controller with regard to the direct offer of information society services. The data subject's intention to ban the exercise of the abovementioned rights must be unambiguous, specific, free, and informed. The ban may apply to exercising some of the rights mentioned above. The data subject can revoke or amend the ban at any time. The ban shall not result in detrimental effects to the exercise by third parties of property rights arising from the data subject's decease or of the right to defend a legal claim.
- **Special categories of personal data**: article 107 of the Code provides that consent to the processing of special categories of personal data (when used as a legal basis) may also be given in accordance with simplified arrangements approved by the Garante, as set out in the rules of conduct referred to in article 106 of the Code (e.g., codes of conduct and professional practices by private and public entities, including scientific societies and professional associations, which are involved in the processing of data for statistical or scientific purposes), or in the measures referred to in Article 2-*septies* (e.g., a decision by the Garante that takes into account the guidelines, recommendations and best practices published by the European Data Protection Board ('EDPB') and best practices on the processing of personal data). For the sake of completeness, the processing of special categories of personal data should also comply with the general authorizations published by the Garante. In this regard, it should be noted the following:
  - *Processing special categories of personal data necessary for substantial public interest reasons*: article 2-*sexies* of the Code, by addressing the exceptions set forth by article 9(1)(g) of the GDPR, provides that the processing of special categories of personal data for reasons of substantial public interest shall be carried out only if pertaining to the areas indicated in article 2-*sexies*(2) of the Code and it is provided under EU or Italian laws or regulations or general administrative acts.
  - *Processing health data*: article 110 of the Code permits the processing of health data to carry out research in the medical, biomedical, and epidemiological fields without data subject consent (including where research is part of a biomedical or health program under article 12-bis of Legislative Decree no. 502/1992). Such processing is permitted if EU/Italian law or regulation authorizes the scientific

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

research and the controller performs a DPIA which is made publicly available, or if informing data subjects involves disproportionate effort or is likely to make impossible or seriously impair the purposes to be achieved by the research (according to the conditions set forth under the Code). In the latter case, article 110 of the Code (as amended by Decree-Law No. 19/2024) provides that it is necessary to receive the positive opinion of the competent ethics committee and the guarantees identified by the Garante pursuant to article 106(2)(d) of the Code must be observed.

Finally, article 110(2) of the Code provides that if, in such circumstances, controllers processing personal data receive a data subject rectification or completion request pursuant to article 16 of the GDPR, they must record the request without modifying the data if the rectified or completed data do not produce significant effects on the research outcome.

- *Processing of genetic, biometric, and health data*: article 2-*septies* of the Code provides that the processing of genetic, biometric, and health data shall be carried out only if both the processing complies with article 9(2) of the GDPR and certain security measures (such as encryption, pseudonymization, and minimization) are implemented. Such security measures will be established by the Garante at least every two years. In the meantime, the Garante has: (i) updated the general authorization no. 8/2016 on processing of genetic data; and (ii) issued further guidance on the requirements for processing health data, available on the relevant institutional website. Moreover, the Code prohibits the dissemination of genetic, biometric, and health data, while permitting the processing of biometric data with regard to the procedures for physical and logical access to data by authorized persons, provided that all processing security requirements pursuant to the Code and article 32 of the GDPR are met. Lastly, the Garante adopted on November 12, 2014, the General Application Order Concerning Biometrics. Although the order was issued before the entry into force of the GDPR, it may still provide useful guidance on the processing of biometric data.

- **Public interest**: Article 2-*ter* of the Code provides that personal data may be communicated between controllers for the performance of a task carried out in the public interest or in the exercise of official authority only if either:
  - communication is provided by a law, a regulation or general administrative acts; or
  - communication is necessary to carry out tasks in the public interest or to fulfill institutional duties and the Garante has been previously informed.

Furthermore, pursuant to article 2-*ter* (1-*bis*) of the Code, public administrations, independent authorities, and state-controlled companies are always allowed to process personal data if necessary for the performance of a task carried out in the public interest or for the exercise of public powers granted to them.

- **Processing of criminal conviction and offense data**: article 2-*octies* of the Code provides that the processing of personal data relating to criminal convictions or offenses may be carried out if an Italian law or regulation

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

authorizes the processing and provides appropriate measures to safeguard data subjects' rights and freedoms. Where such provisions are not enacted, requirements for the lawful processing of judicial data shall be determined through a decree of the Ministry of Justice. In this regard, the Garante also published ethical rules on the processing of personal data carried out in order to carry out defensive investigations or to assert or defend a right in judicial proceedings.

- **Processing for archiving in the public interest, scientific or historical research, or statistical purposes**: article 100 of the Code, by addressing the exception set forth by Article 9(1)(j) of the GDPR, permits public entities, such as universities and research institutions, to disclose and disseminate personal data to specified recipients to support science and technological research and strengthen collaboration in certain circumstances. However, this exception does not apply to the disclosure or dissemination of special categories of personal data or criminal conviction and offense data. The Garante's updated general authorization no. 9/2016 on processing personal data for scientific research purposes sets out requirements for universities, research institutes, health professionals, health organizations and other specified persons that process personal data for scientific research purposes. The Garante also adopted the following ethical rules for processing personal data for archiving in the public interest, scientific or historical research, or statistical purposes:
  - ethical rules for processing for archiving purposes in the public interest or for historical research purposes;
  - ethical rules for the processing for statistical or scientific research purposes carried out within the Italian National Institute of Statistics; and
  - ethical rules for processing for statistical or scientific research purposes.

3. Principle relating to the processing of personal data

Article 5 of the GDPR outlines seven key principles related to the processing of personal data. These principles are particularly important to small- and medium-sized enterprises (SMEs), especially in their capacity as data controllers, determining the purposes and means of processing personal data. The principles that SMEs must adhere to when collecting and processing personal data include:

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability.

These principles are established at the beginning of the GDPR and serve as the foundation for the entire regulation.

Adherence to data protection principles represents the first and arguably most crucial step SMEs can take to ensure compliance with the GDPR and data protection law. Similar data protection principles apply when personal data are processed for 'law enforcement purposes' under the Law Enforcement Directive (LED).

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

A. Lawfulness, Fairness, and Transparency

Personal data processing must be lawful, fair, and transparent with respect to the data subject. Individuals should be thoroughly informed and aware of how their personal data will be collected, used, accessed, or otherwise processed, including the scope of such processing.

The lawfulness of processing personal data necessitates that any such processing conducted by the controller must be grounded in one of the legal bases prescribed in Article 6 of the GDPR.

To ensure compliance with the principle of lawfulness, the controller must establish a specific and appropriate legal basis for the processing activity. The GDPR outlines six legal bases for data processing, and it is incumbent upon the controller to identify and apply the correct legal basis in each instance. Furthermore, the GDPR imposes additional conditions for the processing of special categories of personal data, thereby requiring heightened scrutiny and justification for such activities. Failure to establish and apply a lawful basis results in unlawful data processing, thereby violating the principle of lawfulness as enshrined in the GDPR. Moreover, the processing of personal data by the controller must not involve any unauthorized activities or misuse of the data. This includes but is not limited to engaging in criminal activities, breaching professional confidentiality, abusing legal authority, infringing copyright, violating contractual obligations, or contravening applicable laws and regulations.

The GDPR contains specific rules on transparency obligations in Articles 12, 13, and 14. These rules outline the types of information that must be provided to data subjects and how it should be provided.

For SMEs to uphold transparency, they need to ensure that the method of conveying information is well-suited to their platform and target audience. Fair and transparent processing principles necessitate informing individuals about the existence and purposes of processing operations. This is particularly important in situations where individuals can choose whether to use a particular service or product and enter into a business relationship with the controller (for example in the case of processing based on consent and a contract). If individuals know, before entering into a business relationship with a controller, who processes their personal data, how their data is handled, for what purpose and to whom their data are disclosed, they will be able to make an informed decision as to whether to enter into a business relationship with the controller or to try to renegotiate the terms of that relationship.

There are situations where personal data has not been collected directly from the data subject. This includes personal data obtained by the data controller from sources such as third parties, publicly available sources, data brokers, etc.

If individuals are not informed that their data are being collected and processed, they have no control over their data and cannot exercise their rights.

1. Example

The recruitment agency uses an algorithm for automated decision-making and profiling. The individual gives consent to the employment agency to use his/her personal data for the purpose of profiling. Individuals start receiving job offers that are not in line with their qualifications, work experience and expectations. As a result, the individual begins to suspect that something is wrong with the algorithm, even though the controller has not informed him in plain and clear language that there is a risk that the processing of his or her personal data for the purpose of profiling could adversely affect his/her

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

interests. It is considered that the type of processing described would not comply with the principle of fairness.
Controllers may not process personal data in secret and data subjects should be aware of the potential risks.

2. Example

The organization/company has installed video surveillance, and the processing is based on legitimate interest. Video surveillance is installed at the premises of the organization/company: reception and corridors and in the kitchen; however, the employer (controller) did not inform the employees that video surveillance had been installed, so the conduct mentioned above does not comply with the principles of fairness and transparency. The controller has a legal basis for the processing but has not informed the data subjects that they are being recorded.
Personal data may sometimes be used in a way that adversely affects the individual, but if the reasons are justified, such conduct would not be considered unfair.

3. Example

An individual uses a shuttle service on a bus without purchasing a transport ticket. The bus ticket controller asks the individual to show his/her identity card and prescribes the necessary information from it to issue a fine. The processing of personal data in the situation described is necessary for the exercise of the controller's official authority and is considered fair even though it has a negative impact on the individual.
For online services, the characteristics of services, applications, and products must be explained to data subjects so that individuals can truly understand how their data is handled.

4. Example

A social media service provider collects and processes the personal data of its users in order to provide the service, as well as for marketing purposes, which means that it transfers personal data to third parties to target advertising. In its privacy notice, the social media service provider (data controller) clearly states that users' data is transferred to third parties to target advertising. In other words, a social media provider sells and benefits from individuals' personal data. In cases where a social media service provider gives the user (data subject) the opportunity to give or refuse consent to such processing and to provide the user with information on how his or her data will be handled and shared for targeted advertising, this processing of personal data shall be deemed to comply with the principle of fairness.

B. Purpose Limitation

The purpose limitation principle requires that personal data be collected and processed exclusively for one or more legitimate purposes that are explicitly defined and sufficiently specific.

Secondary usage for a different purpose (in the public interest, for scientific or historical research purposes, or statistical purposes) is permitted if the new purpose is not incompatible with the original purpose, as communicated to the data subject, and where sufficient safeguards are in place.

5. Example

The marketing agency has collected and stored personal information about its customers. Further use of this data by the marketing agency is permitted for statistical

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

analysis of the purchasing behavior of its customers since the processing of personal data for statistical purposes is consistent with the original purpose of collection. A marketing company does not have to provide an additional legal basis, e.g., it does not have to ask individuals for consent. However, for further processing of personal data for statistical purposes, the marketing agency has put in place appropriate safeguards, i.e., pseudonymized personal data of clients.

I. Guidelines

What do SMEs have to do to comply with the purpose limitation principle?
Adhering to this principle not only ensures that businesses (controllers) respect the principles of minimizing data and maintaining reliability but also helps build trust with customers and stakeholders.
This means that data controllers must:

- be evident from the outset why they collect personal data and for what purposes;
- comply with transparency obligations to inform individuals of the purposes of the processing;
- If the data controller intends to process personal data for a purpose other than or different from the specified purpose, the controller must ensure that the new use is fair, lawful, and transparent.

If the purposes of the processing change over time, or if the controller wishes to use the data for a new purpose that was not originally intended, this can only be done if:

- the new purpose is in line with the original purpose;
- the individual gives special consent for the new purpose; or
- The data controller may establish a legal provision requiring or allowing new processing in the public interest, such as a new function for a public authority.

If the new purpose for data processing is deemed compatible with the original purpose, the data controller is not required to establish a new legal basis for further processing. However, if the data was initially collected based on consent, the controller is generally required to obtain fresh consent to ensure that the new processing remains both fair and lawful. Additionally, the data controller must update its privacy information to maintain transparency with respect to the data subjects concerning further processing.

What if an undertaking (the data controller) wants to process the collected data for another purpose?
Any new use of data that is not in line with the original purpose must have its legal basis and cannot be justified by the fact that the data was initially collected or processed for a different legitimate purpose. The processing is restricted to the originally defined purpose, and each new purpose will require a separate legal basis. For example, sharing personal data with third parties for a new purpose will need to be carefully considered, as such sharing will likely require an additional legal basis separate from the one for the initial data collection.

6. Example

An air carrier collects data from its passengers for the purpose of booking and issuing boarding passes and air tickets to passengers. The air carrier is required to disclose personal data of individuals to immigration authorities, which are then used for immigration control purposes, which differ from the original purpose of data collection. To disclose personal data to immigration authorities, the air carrier will have to establish a separate legal basis.
This principle is fundamental in the context of consent, in which different purposes cannot be combined and granularity occurs. Depending on the scope and purpose of the

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

data processing activity, the data controller must choose the appropriate legal basis and should not confuse the different purposes of the data processing.

7. Example

A retail store collects personal data from its customers to include it in the loyalty program. The individual gives consent to the processing of his/her personal data for membership in the loyalty program in order to receive some discounts. However, although he/she has not given his/her consent for direct marketing purposes, he/she began to receive promotional materials and advertisements in his mailbox and email address after some time. The processing of personal data for direct marketing purposes is not in accordance with the original purpose, so the retail store must request the client's consent for direct marketing purposes.

The main takeaway from the above cases

Determining the purposes before collecting personal data helps data controllers be responsible for their processing activities. It also helps individuals understand how and why companies (controllers) use their data. This may also impact their decision to want or not to enter into a business relationship with a company, whether they want to consent to the processing of their data, and helps individuals exercise their rights more easily.

C. Data Minimization

Data minimization is a fundamental principle that underpins both the principles of purpose limitation and storage limitation. Under the GDPR, the standard has been refined to "adequate, relevant, and limited to what is necessary."

Data minimization also helps protect personal data by restricting the amount of information at risk in the event of a breach.

Organizations must assess this based on the specific circumstances of their processing operations. If the data are not necessary for the controller's processing purposes, the controller should refrain from processing the personal data. In addition, data that is no longer necessary for the purposes for which it was collected and that do not have specific retention rules, such as medical records, must be erased or anonymized as soon as possible, even without the individual's request for "erasure."

8. Example

An individual wants to become a member of a city library. To this end, at the desk, they asked him/her to fill in a form containing the personal data necessary to become a member of the library: first name, surname, address, date of birth, ID number, information about education, and a gas or electricity utility invoice. He/She must also provide a photo.

For the data minimization principle, it is excessive to ask an individual for information about his/her education and utility invoice in order to become a library member unless this is not connected with other information that the library needs to process (for example, to double-check the address via the invoice, understand the purpose of the visit to the library, or the kind of collections that the person wants to consult).

II. Guidelines

What amount of data is considered appropriate and relevant?

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

As the GDPR does not define the amount of personal data that is considered "adequate, relevant and limited.", controllers will have to assess this information based on the circumstances of their planned processing operations.
SMEs should regularly assess the type and amount of personal data they handle, making sure that the data they process continues to be appropriate, pertinent, and indispensable. The controller must collect and retain only a minimum amount of data for special category data or criminal offenses.
SMEs shall periodically review their processing activities to ensure that the personal data they process remains relevant and appropriate for their purposes and that they delete anything they no longer need. This is closely linked to the principle of storage limitation.
SMEs should not collect, store, or process in any other way more personal data than they need to achieve the purpose, and the personal data they process should not include non-essential details. Furthermore, by introducing technical safeguards aimed at ensuring that only personal data that are necessary for a specific purpose are collected and used, it is sometimes possible to avoid using personal data or to use measures to reduce the possibility of attributing data to a data subject (for example, pseudonymization).

D. Accuracy

Under this principle, businesses must guarantee the accuracy and timeliness of personal data. The accuracy principle is a legal obligation of the data controller, but it is deeply interconnected with the rights of erasure and rectification in the case of inaccurate data.

SMEs should, for instance, make every effort to promptly correct or delete inaccurate personal data, considering the purposes for which the data are used. It is a straightforward requirement that all personal data collected, stored, or processed by an SME must be accurate and current. All necessary measures must be taken to promptly correct any inaccuracies, including evaluating the need for periodic updates to any personal data held by an SME.

It is important for SMEs that handle personal data to establish clear procedures for rectifying or deleting any inaccurate personal data as part of their data management activities. The specific measures SMEs must take to ensure the accuracy of personal data will vary depending on the circumstances, especially the nature of the personal data and the processing involved. SMEs must also be mindful of their responsibilities regarding data subjects' right to rectification, which includes rectifying or completing inaccurate personal data.

It is essential to promptly rectify any inaccuracies by taking all necessary measures, including periodically updating any personal data held by the data controller.

The controller is responsible for ensuring the accuracy of the personal data it collects. This involves accurately recording the information provided and its source, as well as taking appropriate steps to verify and maintain the accuracy of the information.

9. Example

When an employee receives a raise, the employer must update the employee's salary records accordingly.

10. Example

A buyer changed his address. A retail store selling its products to the customer needs to update the buyer's address in order to deliver the products to the correct location.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

In some cases, it is reasonable to rely on the individual's statement that the personal data have changed, for example, when changing the address or other contact details. In line with good practice, it is from time to time to ask individuals to update their personal data. However, if an individual notifies an organization or company of a new address, the organization or company should update its records.

11. Example

An individual changes his address and informs his telecommunications provider of the new address to send invoices to a new address. The telecommunications service provider shall immediately correct the address in its information systems. There may be situations where the data controller suspects that the individual (customer) is not telling the truth. In such cases, it would be reasonable to ask the individual for proof, such as proof of residence.

12. Example

An individual wants to conclude a loan agreement with a credit card company. The credit card company checks the creditworthiness of the individual against special available databases containing data on the credit obligations of natural persons. The database contains unclear and outdated data on the individual's debts and unpaid accounts. For this reason, the individual suffered negative effects because the credit card company refused to issue him a credit card. Controllers of such databases must, therefore, make particular efforts to comply with the principle of accuracy.

Where a natural person requests the rectification of his or her personal data, the controller should consider whether the information is correct, and, if this is not the case, the controller should delete or correct it. However, individuals do not have the right to erasure solely because the data are inaccurate. However, the principle of accuracy requires the controller to take all reasonable steps to erase or correct inaccurate data without delay, and in some cases, it may be reasonable to erase the data.

13. Example

The individual was misdiagnosed and asked the doctor to correct it. It is in the best interest of the individual that misdiagnosis is maintained as part of the individual's medical documentation, even after correcting the diagnosis, as it is relevant to the treatment of the individual and his/her other health problems.

14. Example

The construction company employs new employees. During the job interviews for all jobs (including in the office and on the construction site), the employer asks specific questions about the health situation that are relevant only to construction site workers. It is excessive to collect such personal data for an individual who has applied for employment in the workplace, for example, an administrative assistant.

Main takeaway

It is important that the controller does not process more data than is actually necessary to achieve the purpose, otherwise such processing is very likely to be unlawful and will also constitute a breach of the principle of data minimization.

E. Storage Limitation Principle

Storage limitations require controllers to manage the lifecycle of processed personal data, removing it when the purpose is fulfilled and processing is no longer relevant.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

For instance, SMEs are required to retain personal data in a manner that allows for the identification of individuals only for the duration necessary to fulfill the purposes for which the data were originally processed. However, personal data may be stored for extended periods if the data are to be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, in accordance with the GDPR, provided that appropriate technical and organizational measures are in place to safeguard the rights and freedoms of the individuals concerned. Consequently, SMEs should generally ensure that personal data are deleted as soon as they are no longer necessary for the purposes for which they were initially collected.

To this end, the GDPR recommends that the SME establish time limits for erasure or periodic review. SMEs should also ensure that individuals are aware of retention periods or the criteria used to calculate them. SMEs storing personal data offline or in manual form in a filing system, even where digital versions or copies have been deleted, must still have justifications for retaining this personal data in an offline form and responding to data subject requests.

III. Guidelines

Controllers should generally erase personal data as soon as they are no longer necessary for the purposes for which they were initially collected. The controller should set deadlines for erasure or periodic review.

Controllers should implement clear policies on retention periods and erasures. The retention policy should consist of the categories of personal data processed and the retention period for each category of personal data.

In certain instances, particularly when small organizations or companies engage in occasional low-risk processing of personal data, they may not require a retention policy. However, it is essential to consistently assess the processed data. Data that is no longer essential should either be deleted or anonymized. While it may not always be feasible to completely erase all traces of data, it is always possible to render the data unusable. When controllers remove personal data from information systems, they should also ensure that such data is deleted from the system's backups.

How can businesses know how long they can store personal data?

The GDPR does not prescribe how long data should be stored; it depends on the legal basis for the processing. However, regulations do define this; for example, labor regulations define how long the employee’s data should be stored.

In cases where there is no legal obligation to keep the data, the controller should determine how long it will be stored and should be able to explain why it holds the data. Personal data should be kept for as long as the purpose(s) for which they are collected and processed exist, but the data cannot be kept “only in case” the data controller sometimes finds the purpose of their use in the future.

Depending on the circumstances, it may also be more appropriate for the controller to anonymize the data once it is no longer necessary to identify or identify the individual. The data are indeed anonymous and therefore no longer “personal” data, only if the individual is no longer identifiable. However, if the data could still be attributed to the individual through the use of additional information, they would only be pseudonymized and would, therefore, continue to be considered personal data. If the procedure applied to the allegedly anonymized data is not permanent and can be invalidated, the data are not anonymized.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION’S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

F. Integrity and Confidentiality

The principle of integrity and confidentiality requires the controller to handle personal data in a manner that guarantees a suitable level of security and confidentiality. This includes safeguarding against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. To fulfill this requirement, the GDPR mandates that data controllers must implement appropriate technical and organizational measures (hardware, software, authentication measures, manage authorization, etc.). In essence, data controllers must ensure that their security measures safeguard against both accidental and intentional harm, loss, or unauthorized disclosure of the personal data they handle.

The GDPR does not specify the security measures SMEs should implement, as technological and organizational best practices constantly evolve. SMEs should consider various options to determine the most appropriate measures under the circumstances, as there is no "one size fits all" approach to data security.

15. Example

A bank owns the personal data of an individual who is a bank client. If the client decides to close the account, the bank must retain his personal data for the period prescribed by law. Data controllers should always take into account legal or regulatory requirements. There are different legal requirements that prescribe how long the data should be kept, for example, such information may be necessary for income tax or audit purposes. Or, for example, there is a law that determines how long medical records should be kept in health institutions. If controllers store personal data in order to comply with legal requirements, this will not be considered a breach of the principle of storage limitation.

16. Example

A Debt Collection Agency possesses the personal data of an individual who has debts in the bank. The Agency tries to collect debts on behalf of the bank and must have some information to contact the individual in connection with the debt recovery. Once the debtor has settled the debt, there is no purpose for the debt collection agency to keep his data.

17. Example

A gas station installed video surveillance to protect people and property. It has introduced a retention policy and keeps the recordings for three months, after which the records are deleted. One robbery happened at a gas station. The crime has been reported to the police, and the service station will have to retain the recordings longer than the prescribed storage period to conduct the investigation.

18. Example

An individual bought 5 cosmetic treatments in a beauty salon. The individual gave his/her phone number and e-mail address so that the salon could contact him in case of any changes regarding the date of the contracted treatment and remind him by sending a message. When the individual uses all the treatments he paid for, the beauty salon should no longer keep information about the individual.

19. Example

When ordering flowers from the flower shop, a person gives the name, telephone number, and address of the person to whom the flower must be delivered. After the flower delivery, the flower shop can no longer store the personal data of the person to whom the flowers were delivered.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

20. Example

An individual has applied for a job. He didn't get a job. The company must keep its data for the period during which a claim relating to the recruitment procedure can be lodged. If a company wants to keep the CV of an applicant for employment CV in its database in order to inform him of a possible job offer in the future, it must request the individual's consent.

21. Example

An individual has entered into a contract with a telecommunications service provider. The contract ends after 12 months. Personal data of individuals (name, surname, ID number, address, email address) are kept for 12 months. However, traffic data are kept in accordance with the Electronic Communications Act. Also, the data are not deleted within 12 months, if the user has filed a complaint against the telecommunications service provider, in this case, the data will be kept until the request is resolved in accordance with the regulations. Likewise, an individual's data will not be deleted if the data controller has to take enforcement measures in case of non-payment.

IV. Guidelines

How can the company check whether the safeguards are effective and adequate?
The data controller can verify whether the security measures implemented are effective using a range of techniques, such as vulnerability scanning and penetration testing. In this way, the controller can test its information systems to detect risks and vulnerabilities that need to be eliminated and mitigated. Test results should be documented, and recommendations should be followed up on to implement appropriate safeguards. Failure by controllers to take proper safeguards could lead to serious consequences for individuals, such as identity theft, fraudulent credit card transactions, or in some cases, even lives could be endangered, such as witness identification or ransomware attacks in hospitals.
For these purposes, controllers must ensure the resilience of their systems and services. This means that systems can continue operating under conditions caused by a physical or technical incident, and data controllers must be able to restore the system to its normal state.

22. Example

The e-citizens system provides an additional level of data security for the services it offers through two-stage authentication. In addition to entering a personal password, users must fill in a second application to access their account. When citizens want to access their personal account, for example, to obtain a certificate of impunity, the e-citizen system sends a security code to a mobile number linked to a personal account (for example, an OTP). In this way, a two-step check provides better protection of personal data against unauthorized access to personal accounts through hacking.

23. Example

A company participates as a partner in the EU project. The company was asked to send the lead partner (project coordinator) the CVs of the employees who will participate in the project. Although sending a CV via email is not a safe way to send personal data, the company cannot find another solution, sending CVs via email in a compressed file and sending a strong password to open a CV file to the project manager's mobile phone number.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

In many cases, data breaches are due to the theft or loss of equipment, the loss of old computers, or printed records that have been lost, stolen, or misappropriated. Technical measures must include physical and cybersecurity measures.

G. Accountability

The accountability principle addresses the data controller as the focal point of responsibility, accountability, and liability regarding compliance with the principles of the GDPR.

The principle of accountability presents an opportunity for each data controller to demonstrate their respect for individuals' privacy. This benefits their business and enhances the organization's reputation and competitiveness in the market. By upholding the principle of accountability, data controllers can effectively show that they have proactively assessed risks and implemented necessary safeguards and security measures in cases of personal data breaches or infringements on individuals' rights. Failure to demonstrate compliance with this principle could result in fines and damage to the organization's reputation.

Within an organization, staff whose job is to support the controller in its coordination efforts, including a data protection officer, a compliance officer or a team leader, may be appointed. Where the controller relies on specific staff to encourage compliance by a wider organization, it should of course ensure that these staff are trained and receive the resources necessary to carry out this task. Whether there is support staff or not, compliance with data protection should be considered to be the responsibility of all employees.

H. Data Protection by Design and by Default

Data protection by design and by default is an essential component in upholding the principle of accountability. It involves embedding data protection into all data processing activities.

Implementing data protection by design and by default means that prior to commencing the processing of personal data, businesses should design the data processing operations in compliance with data protection law. Controllers are mandated also to integrate data protection by design and by default continuously throughout the processing phase by regularly assessing the effectiveness of the established safeguards.

24. Example

A dental polyclinic (the data controller) opted to install parking bollards at the parking entrance due to the unauthorized use of parking spaces by individuals from other organizations.
The dental clinic engaged an organization to install parking bollards in the parking lot, which requested vehicle registration plates from the polyclinic. They stated that the license plate numbers were necessary to create stickers for employees to affix to their windshields. These stickers would be scanned as the vehicle approached the parking.
Upon review, the dental polyclinic determined that the system for parking bollards did not require the collection of vehicle license plates or any other personal data from its employees. Instead, providing unique stickers to employees, instructions on usage, and prohibitions against sharing with third parties sufficed.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

In this scenario, the polyclinic applied for data protection by design and by default by collecting only the data essential to fulfill the purpose. This action also aligned with the principles of data minimization and accountability.

25. Example

A company specializing in product distribution sought to evaluate the efficiency of its deliveries in terms of delivery time, workload scheduling, and fuel consumption. To achieve this, the company processed personal data of drivers and customers, a practice that could potentially lead to monitoring customer habits and encroachment on employee privacy. To mitigate these risks, the company pseudonymized customer and employee personal data. This approach reduced the likelihood of data breaches and enabled the company to achieve its data collection purpose while adhering to the principle of data minimization.

26. Example

A software development company is creating a client's new customer relationship management (CRM) system. The CRM system will handle sensitive customer data, including contact information, purchase history, and communication logs.
To ensure data privacy and security, the software development company implements privacy by design and default principles throughout the development process. They consider data protection from the initial design phase to deployment and ongoing maintenance.
During the design phase, the company incorporates privacy features such as granular access controls, encryption of sensitive data at rest and in transit, and regular security audits. They also implement mechanisms for data minimization, ensuring that only necessary data is collected and stored.
In addition, the company integrates privacy by default by setting strict privacy settings as the CRM system's default configuration. This includes enabling privacy-enhancing features like anonymous browsing options, opt-in consent mechanisms, and automatic data deletion policies for outdated information.
By embedding privacy protections into the CRM system's design and default settings, the software development company ensures that customer data is handled securely, in compliance with data protection regulations, and with respect for user privacy rights.

Check more cases and guidelines at the end of the handbook.

4. Lawful Basis for Processing

Personal data processing is only lawful if permitted under EU data protection law. Therefore, controllers must be able to base their processing on a specific case of lawfulness so that the activity they carry out is not to be regarded as unlawful precisely.

Personal data processing encompasses any operation on personal data conducted by an organization, including sharing, storing, recording, and exchanging activities.

One of the initial questions that SMEs acting as data controllers should ask themselves before commencing data processing is: “What is my reason or justification for processing this personal data?”.

This is a crucial question because all personal data processing must be lawful and have a “legal basis.” Article 6 outlines the potential legal bases, which include consent, contract, legal obligation, vital interest, public task, or legitimate interests.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

With regard to the processing of **special categories of data**, as mentioned, Article 9, Paragraph 1, opens with a general prohibition on their processing. The special category of personal data includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning an individual's sex life or sexual orientation. The prohibition of processing may be overridden if one of the exceptions provided for in paragraph 2 applies. For any processing of personal data that is necessary, proportionate, and appropriate, a legal basis can be identified only within the exceptions provided. Article 9 is to be applied in coordination with Article 6. It is also provided that for the processing of genetic, biometric or health-related data, Member States may maintain or introduce further conditions or restrictions.

As a general rule, **the legal basis must be communicated to the individual** when the processing begins, or within a reasonable timeframe, and no later than one month after obtaining the data (if the data has not been obtained from the individual.

A new element of the GDPR is Article 8, which provides for the possibility that minors may express valid consent if they are at least 16 years old (the national legislator can reduce this to 13) with regard to the direct offer of "information society services." For this, see also the specific rules provided by national legislation.

27. Example

You are an SME operating a retail store. You want your employees to wear name tags so customers would feel more comfortable. Name tags allow customers to address employees by name, creating a more personal and friendly interaction. This can make the shopping experience feel less impersonal and more welcoming. In this case, consent would not be applicable because employees might feel pressured to give consent, scared of adverse consequences (i.e., getting fired). A retail store could rely on legitimate interest, provided that it proves its legitimate interest by conducting a balancing test (LIA).

V. Guidelines

The following is a list of elements to be borne in mind for the legal basis.

a. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

b. You must have a valid lawful basis in order to process personal data.

c. Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

d. You must determine your lawful basis before you begin processing, and you should document it. We have an interactive tool to help you.

e. Take care to get it right the first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.

f. Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

g. If your purposes change, you need to consider whether you need a new lawful basis.

h. If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

i. If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
j. Consent is not required for every data processing! For example, if you employ a person and according to the labor regulations you have to register your employees for mandatory health and pension insurance. Therefore, you do not need to collect employees' consent to share data with the competent national authorities.
k. If there is an imbalance in the relationship, in the sense that one party is in a more favourable position than the other or in a relationship of dependence towards another, it is unlikely that consent, in that case, can be freely given.
l. Having invalid consent is the same as not having it at all.

Olivia can help you to identify the lawful basis for the processing of personal data.

A. Consent

Article 7 provides the "Conditions for Consent". It states that when processing is based on consent, the controller must be able to demonstrate that the data subject has provided consent for the processing of their data. This requirement pertains to the "burden of proof".

In addition, if the data subject's consent is provided within the context of a written declaration that also addresses other matters, **the request for consent must be presented in a manner that is clearly distinguishable from the other matters**, in **an intelligible and easily accessible form, and using clear and plain language**.

Any portion of such a declaration that infringes upon the provisions of the Regulation shall not be legally binding. The controller must ensure that consent is not obscured within overly complex or lengthy privacy policies, that it is "easily accessible" in its format (considering the user interface), and that it employs clear and plain language. Consent embedded within an elaborate and incomprehensible "Terms of Service" that effectively implies consent is not considered valid under the GDPR.

Technically, data subjects can provide consent through a statement, whether written, oral, video, or audio, or affirmative action, such as clicking a button or typing a digit. The GDPR does not prescribe a specific form for obtaining consent, allowing it to be obtained electronically. Nevertheless, the data controller must demonstrate that the data subject has indeed consented.

To be valid, consent must be freely given, informed (indicating the possibility to withdraw), specific, and unambiguous in indicating the data subject's wishes to have his/her data processed.

If consent is part of the terms and conditions or used in a power imbalance situation (e.g., in an employment context), it is assumed not to have been **freely given**.

Informed consent means that data subjects must understand what they agree to. Therefore, data subjects need to be given information concerning the identity of the controller and the purposes of the processing, the type of personal data that will be processed, and the existence of the right to withdraw consent. Indeed, the data subject retains the right to withdraw their consent at any time.

Withdrawing consent does not affect the lawfulness of processing based on consent before its withdrawal. The data subject must be informed of this right before

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

providing consent, and the process of withdrawing consent must be as straightforward as giving consent. This implies that if consent is provided by ticking a box, the data subject must be equally straightforward to withdraw consent by unticking the box. The consent is only considered valid if the process of withdrawing consent requires navigating through complex and obscure website sections. When evaluating whether consent has been freely given, particular attention must be paid to whether the performance of a contract, including the provision of a service, is made conditional on consent to the processing of personal data that is not essential for the fulfillment of that contract.

Specific consent means that if the data processing is performed for several purposes, consent must be obtained for each purpose. This is called the granularity of consent.

Unambiguous means that it must be evident that the data subject has consented to the particular processing. Actions such as scrolling or passing through a web page cannot be considered affirmative actions (unless the user is asked to draw a figure with the cursor to give consent or the like), as they cannot be distinguished from other forms of interaction with the web page.

Due to their age and maturity, **children** may need to be made aware of the risks. Therefore, every organization/company that processes children's data must be aware of this fact and these risks. When providing information society services to children on the basis of consent, the organization/company must make reasonable efforts to verify the age of the user or implement systems to verify the age of the user (child).

VI. Guidelines

If you ask a person for consent, you must provide them with sufficient information about the operations regarding their data processing. Otherwise, it will not be considered valid consent. Therefore, you must give the person from whom you seek consent with information about the following:

- who you are (information about the organization/society);
- the reasons for the processing of data based on consent;
- the type of personal data requested;
- the right to withdraw consent at any time (this is a MUST);
- possible risks, safeguards, and automated processing (if any).

Please ensure that the language and vocabulary used are tailored to the specific group consenting to processing personal data (e.g., language used for children should differ from that used for adults). The information should be communicated clearly and plainly so that all individuals can easily understand it.

To make unambiguous consent, bear in mind these four golden rules:

- Consent must be an explicit and confirmatory acceptance.
- Consent can be obtained by recording an oral statement
- Pre-checked consent boxes cannot be valid
- An individual's silence cannot be considered evidence that he or she has consented to the processing of his or her personal data.

Using consent as a legal basis for processing personal data is not always possible or desirable. Demonstrating that consent was freely given, informed, specific, and unambiguous can be pretty challenging. In addition, consent can be withdrawn at any time. SMEs should consider using other legal bases where these would be appropriate.

Olivia can help you draft the consent template.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

B. Contract as a Legal Basis for Data Processing

In some instances, the processing of personal data is necessary for performing (or entering) a contract to which the data subject is a party. The legal basis of "contract" (also known as "contractual necessity" or "contractual performance") is frequently used for the processing of personal data in situations where there is a contractual relationship between the data subject and the controller.

In an online setting, this could be applicable in cases where, for instance, a data subject shares their postal address to determine if a specific service provider operates in their area or when the processing is part of an online service registration process. It's important to note that this concept of preliminary processing does not include unsolicited marketing or other processing conducted solely at the controller's initiative or at the request of a third party, as this isn't carried out at the data subject's request.

Processing personal data based on a contract must be essential for fulfilling the contract. This implies that we cannot rely on contracts to process personal data unless it is indispensable for fulfilling the contract. Additionally, the individual whose personal data is being processed must be a party to the contract.

28. Example

An SME operates an online store and sells products. If a customer contacts the company because they received a different product than what was agreed upon (e.g., incorrect shoe size or color), the processing of the customer's data to resolve this issue could be based on the contract.

29. Example

In an online shop, processing customer information, such as addresses, is essential for fulfilling the delivery of products. The legal basis for this processing would be the performance of the purchase contract between the shop and the customer. The necessity of processing an address is clear in this situation, but other types of information may also be considered necessary for the contract under specific circumstances, such as verifying a customer's age when purchasing alcohol.

30. Example

An online service provider creates a function that allows its users to invite non-members to join the service. Where such an invite is sent, the company collates all the information it holds on the person invited (the invitee) in order to assemble a preliminary profile of their connections to other users, to encourage them to sign up. Since the invite has been sent at the request of a third party (the original user sending the invite), the data subject profiled (the invitee) has not asked the controller to take any steps, and therefore the company cannot legitimately rely on Article 6, Paragraph 1, letter b) as its basis for this pre-contractual processing.

31. Example

A customer goes into a clothes shop to buy a new jacket. The shop doesn't currently have their stock size, but agrees to order it and contact the customer once it is ready. The customer pays for the jacket and provides their contact details so they can be contacted once it has arrived. The shop then uses the contact details and purchase information to create a loyalty card and online profile for their customer to use, which they inform them about when they come back into the shop, much to the customer's surprise. In this case, the terms of the contract of sale between the parties do not support the conclusion that

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

creating a loyalty card or profile is reasonably necessary to perform the contract as entered into.

Further information

When relying on a contractual legal basis for processing personal data, controllers must ensure compliance with other relevant laws governing contractual relationships. This includes verifying that the data subject, particularly if a child or someone with limited capacity, can legally enter into a contract. Additionally, the validity and enforceability of the contract and its clauses must be confirmed. If the processing of personal data is not necessary for contract performance, controllers must consider alternative legal bases or determine if any legal basis is available. Importantly, controllers should not rely on consent as a legal basis if it is made a condition of the contract. When processing sensitive "special category" data as part of a contract, controllers must not only have a valid legal basis but also meet an exception under Article 9, Paragraph 2, such as the data being made public or processing being necessary for legal claims.

C. Compliance with a Legal Obligation

In certain instances, the processing of personal data is required for the data controller to fulfil a legal obligation. This obligation may arise from either EU or Member State law. The law will dictate the purposes of the processing, the criteria for identifying the controller, the type of personal data to be processed, the data subjects involved, and the entities to which the data will be disclosed. Generally, if an SME is legally mandated to handle personal data in a specific manner, the GDPR does not obstruct them from fulfilling that obligation.

Similar to relying on a contract as a legal basis, a controller must assess whether processing is actually 'necessary' to comply with that obligation. If you can reasonably comply without processing the personal data, reliance on this basis will not be appropriate. Controllers are not necessarily required to have a specific legal obligation for the exact processing activity they plan to undertake. However, they should ensure that the overall purpose of processing personal data is to comply with a legal obligation that is clearly based on either common law or legislation. In accordance with the principles of transparency and accountability, controllers should be able to identify the specific law they believe constitutes the legal obligation for the necessary processing. To demonstrate accountability and compliance, controllers may cite specific provisions in legislation, case law, official or governmental advice or guidelines, or other official guidance that outlines the obligations to which the controller might be subject.

It is not necessary for the law to explicitly mandate a specific act of data processing; rather, a law or obligation may serve as the basis for multiple processing operations, provided that these operations are genuinely necessary to comply with the obligation.

32. Example

The employer is required to disclose information about employees' salaries to the state tax administration due to a legal obligation.

How can the employer fulfill this obligation without processing the personal data of the employees? If laws or regulations (delegated legislation based on law) mandate the storage, sharing, or provision of access to specific personal data, then such processing is compliant with the GDPR. The legal basis for processing the data in this scenario is a legal obligation. It's crucial to note that the GDPR does not override the obligations established by national laws or regulations

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

D. Vital interests of Data Subjects or of Another Person

In certain cases, processing personal data is necessary to protect the vital interests of data subjects or another person. This legal ground allows processing in situations of life and death, where the right to personal data protection is overridden by the right to life (e.g., emergency medical care). Since this data processing basis will almost never be in use in the case of data processing by SMEs, it is only mentioned here, and we will not explain this legal basis in detail.

E. Public Task as a Legal Basis for Data Processing

This legal basis is widely used in the public sector. Public authorities are obligated to fulfil their legal duties. For example, the employment office may summon unemployed individuals for interviews as part of their public mandate, and the court may request specific information in legal proceedings that you are required to provide, as the court has the authority to request such information. This legal basis encompasses the processing of personal data that is necessary for carrying out a task in the public interest. For instance, processing personal data for scientific research may rely on this legal basis. Therefore, "public interest" should not be taken to mean, "it would be generally good for the public if this processing happened," but rather that there is a defined public interest that can be identified as a legal basis.

Typically, this legal basis may not apply to SMEs' processing of personal data. However, organizations should be mindful of this legal basis for processing personal data, as there may be instances where they are required to collaborate with public authorities or receive requests for personal data provision from a public authority.

F. Legitimate Interests

In some situations, processing personal data is required for the legitimate interests of controllers or third parties, as long as these interests do not outweigh the interests or fundamental rights of the individuals whose data is being processed.

The legal basis of "Legitimate interests" is a versatile legal basis for processing personal data. It may apply in circumstances where processing operations do not neatly fit into any of the other legal bases; however, it also carries heightened obligations on controllers to balance the legitimate interests they are seeking to pursue with the rights and interests of the data subject.

Controllers who are assessing whether to process data under the legitimate interest legal basis should consider the three elements needed for this legal basis:

a. identifying a legitimate interest that they or a third party pursue;
b. demonstrating that the intended processing of the data subject's personal data is necessary to achieve the legitimate interest; and
c. balancing the legitimate interest against the data subject's interests, rights, and freedoms.

Legitimate interests may serve as an appropriate legal basis in situations where data controllers process personal data of data subjects in a manner that is reasonably expected and has minimal impact on their privacy, due to the nature of the processing or implemented safeguards. However, in cases where the impact on the data subject's privacy rights, or other rights, freedoms, or interests, is more than minimal, it may still be feasible

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

to rely on this legal basis. In such instances, the controller would need to demonstrate a particularly compelling justification for the processing of the legitimate interest.

The legal basis of "legitimate interests" warrants careful consideration as a potential option for controllers. It offers flexibility while also mandating controllers to carefully weigh the interests and rights of data subjects and to implement necessary safeguards and protections.

33. Example

A restaurant offers food delivery services. New clients may enjoy a free meal delivered to their homes. The offer can be activated upon subscription, yet it is limited to one time per household. In this case, the company may check its database of existing clients to confirm that a new client is not from a household that has already benefited from this offer.

34. Example

An online shop requires its customers to share their email addresses to send them updates about the execution of their orders. For this processing, the shop relies on consent. If the shop decides to use email addresses to send marketing materials, this entails a change in the purpose of the processing. Consequently, the shop needs to have a legitimate basis for this new type of processing. The shop provided that the above criteria are met, may invoke the legal basis of a legitimate interest.

Olivia can help you to carry out legitimate interest test

In-depth Analysis: Surveillance

The processing of personal data through video surveillance within the meaning of this Act relates to the collection and further processing of personal data that involves the creation of a recording that constitutes or is intended to be part of a storage system. The processing of personal data through video surveillance can only be carried out for a purpose that is necessary and justified for the protection of individuals and property, taking into account that the interests of the data subjects conflicting with the processing of data through video surveillance do not prevail. The law specifically regulates video surveillance of work premises, video surveillance of residential or mixed residential-business buildings, and video surveillance of public areas (Articles 25-32 of the Law).

It is important to emphasize that monitoring public areas through video surveillance is allowed only to public authorities, legal entities with public powers, and legal entities performing a public service, only if prescribed by law, if necessary for the performance of tasks and duties of public authorities, or for the protection of life and health of people and property.

VII. Guidelines for Legitimate Interest Assessment (LIA)

The Legitimate Interests Assessment (LIA) is a crucial part of determining whether processing personal data can rely on the "legitimate interests" legal basis under data protection laws such as the General Data Protection Regulation (GDPR).

The LIA is subdivided into three main phases:

- Purpose Test: aims to identify the interest that the data controller intends to pursue. The key question is therefore: what in concrete terms (and not just theoretically) is the objective that the data controller intends to achieve in the

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

light of the benefits that he or a third party may derive from it? The interest must therefore be pursued in a way that complies with the legal provisions on the protection of personal data.

- Necessity Test: the purpose of this test is to identify the strict necessity of the pursuit of the interest of the data controller, taking into account the possible harm that would result if he did not carry out the processing. If the objectives were otherwise achievable, by ways and means that would have less impact on the data subjects, the legitimate interest cannot be invoked as a valid legal basis for initiating the processing.
- Balancing Test: the data controller must balance its interests against the interests, freedoms and rights of the data subjects, acting fairly and objectively (fair), expressly assessing the reasonable expectations of the data subject based on his/her relationship with the data controller; the likely impact of the processing on individuals; and the possibility for the data controller to implement measures to mitigate the negative impact on data subjects.

More about video surveillance in Croatia you can find at Olivia-video surveillance modules.

In-depth Analysis: The Cookie Policy

HTTP cookies (also called web cookies, Internet cookies, browser cookies, or simply cookies) are small blocks of data created by a web server while a user is browsing a website and placed on the user's computer or other device by the user's web browser. Cookies are placed on the device used to access a website, and more than one cookie may be placed on a user's device during a session. The web browser stores cookies on the "order" of that internet site, for its further needs. These needs can be different and depend on the purpose of cookies, so for example cookies can collect information about the language the visitor has chosen to display pages at multilingual sites, the sequence of visited pages so that the user can return to the pages in the same sequence, a list of items that the user has inserted into the shopping cart in the online store, up to, for example, the user's IP address, information about the user's successful login to the website, e-mail address, geolocation of the user, whether he is using a computer or a mobile device, which pages of an Internet site he visited, etc.

There are several ways of sorting cookies. They are divided according to duration, according to the source of cookies and according to function. Information from these divisions is important to us when providing information to users regarding the processing of personal data through cookies. Thus, on the basis of information from the section on the duration of cookies, we can provide users with information on the terms of storage of data in cookies, on the basis of information on the source, we can provide information on who all has the right to view the collected personal data and whether personal data is transferred to third countries (countries outside border of the European Union and the European Economic Area) or international organizations, and based on information on the division by function, whether it is necessary to ask the user for prior consent for processing or not.

The GDPR stipulates that if the controller directly collects personal data from the data subject, he or she is obliged to provide information to the data subject at the time of collection (this is the so-called principle of "lawfulness, fairness of transparency"):

- the identity and contact details of the controller,

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

- the contact details of the Data Protection Officer,
- the purpose of the collection/processing of personal data and the legal basis for the collection/processing;
- who has the right to consult the collected personal data,
- whether the personal data are transferred to third countries (countries outside the borders of the European Union and the European Economic Area) or international organizations,
- what is the retention period of personal data,
- the right of the data subject to request access to personal data, rectification, erasure or restriction of processing,
- the right to withdraw consent if consent is the legal basis for the processing,
- whether the data collected is used for automated decision-making.

Examples of cookies that do not require consent

The website provides an Internet store service. To track which items the user placed in the virtual basket, it uses a session cookie to remember the selected items. The session cookie is deleted after the user logs out or makes a purchase. Such cookies fall into the category of so-called "Input by the user" cookies and are collected solely for the stated purpose and do not require consent.
On the other hand, if the same cookies were to be used in addition to the stated purpose and to monitor users' habits for personalized advertising, they would not meet the conditions to be met by cookies for which consent is not required and then unconditioned consent would have to be requested from the user.

The website can display the content of its pages in several international languages and change the design of the content of pages. The website stores this information in cookies to remember the language in which the user wants to view the pages and design the display of page content based on the user's choice. Such cookies also do not require consent.

The website provides e-mail services. So that the authorized user during each of the possible options of the Web e-mail in his e-mail mailbox (checking incoming mail, deleting mail, creating an address book, sending mail,...) does not have to log in again every time, after the first successful login, the website stores the information about the successful authorization of the user in a cookie and uses it for that purpose. Such a cookie also does not require consent.

Consent for the collection of personal data through cookies

For cookies that do not meet the criteria set out in the previous chapter, consent is required for the collection and processing of personal data through cookies.
It is important to note that after loading the homepage of the website and further movement of the user through the pages on that website, no cookie for which consent is required may be stored on the user's terminal equipment until the user has expressly consented to the storage of these cookies. As long as the user has not given explicit consent to the terminal equipment, only cookies that do not require consent may be stored.
Requests for consent to collect data through cookies are usually requested from users via a pop-up window or through a cookie banner that appears on one of the sides of the display of the content of the website, most often at the foot or one of the sides of the display.

Co-funded by the European Union

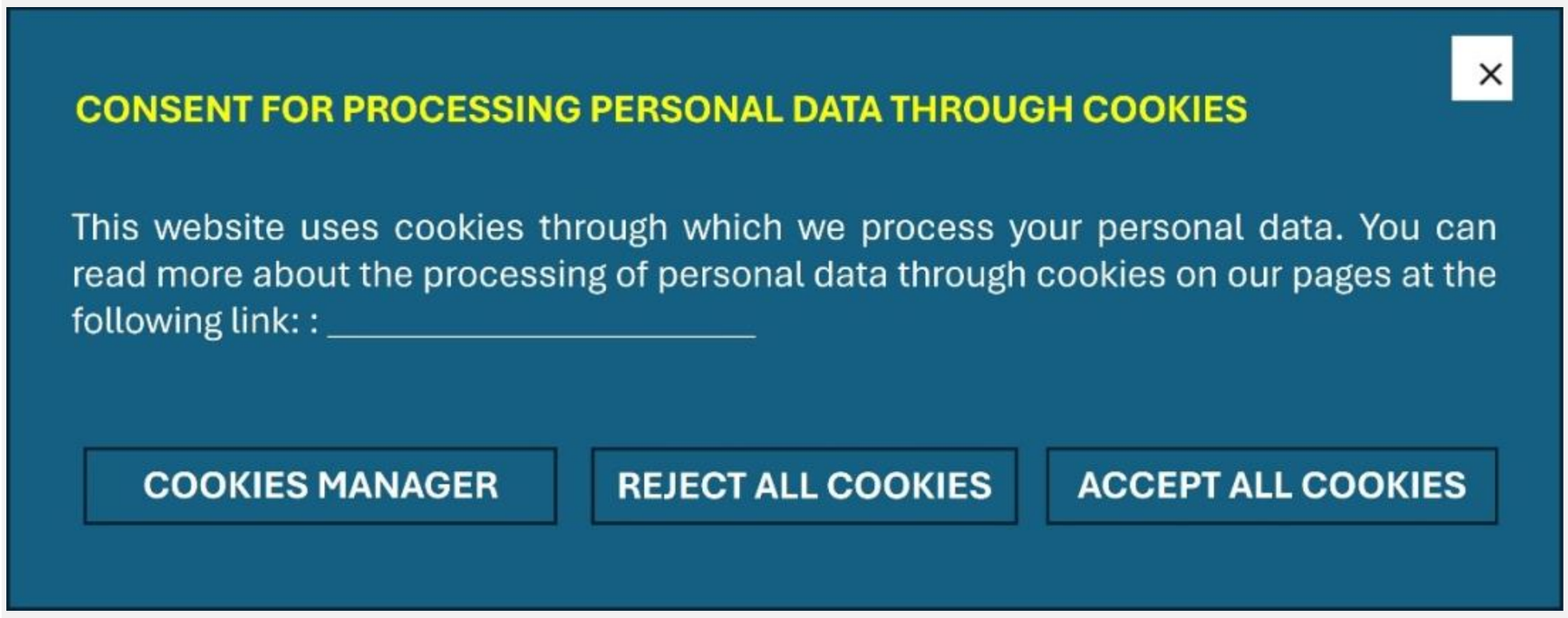
THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

When requesting consent for the collection of personal data through cookies, it is important to note that the General Data Protection Regulation (GDPR) stipulates that consent must not be conditional. The user must be able to explain in clear and plain language what scope of the personal data will be collected and for what purpose and enable him/her to decide whether or not he or she gives his or her consent to the processing of this scope of data. It is also important to note that according to the GDPR consent should be given for each type of cookies according to their functionality separately, i.e. consent for all types of cookies cannot be aggregated.

Example of good practice "Cookie Banner" (first layer)

The data subject is offered options to "Reject all" cookies and "Accept all" cookies and can accept or reject cookies in an equally simple manner, in a single action. By selecting the "Cookie settings" option, the data subject can choose for which purposes they give their consent for processing their personal data through cookies. The first layer of the cookie banner also contains a link to additional information about the types of cookies used on the website and their purposes. By selecting the X mark, the cookie bar closes, and the user can continue to use the website without processing personal data through cookies.

This is an example of a GDPR-compliant cookie banner that provides users with clear choices and information about cookie usage on a website. It emphasizes the importance of giving users equal and easy options to accept or reject cookies, as well as the ability to manage their preferences in detail.



When user chooses option “Cookies manager”, the second layer of cookie banner opens.

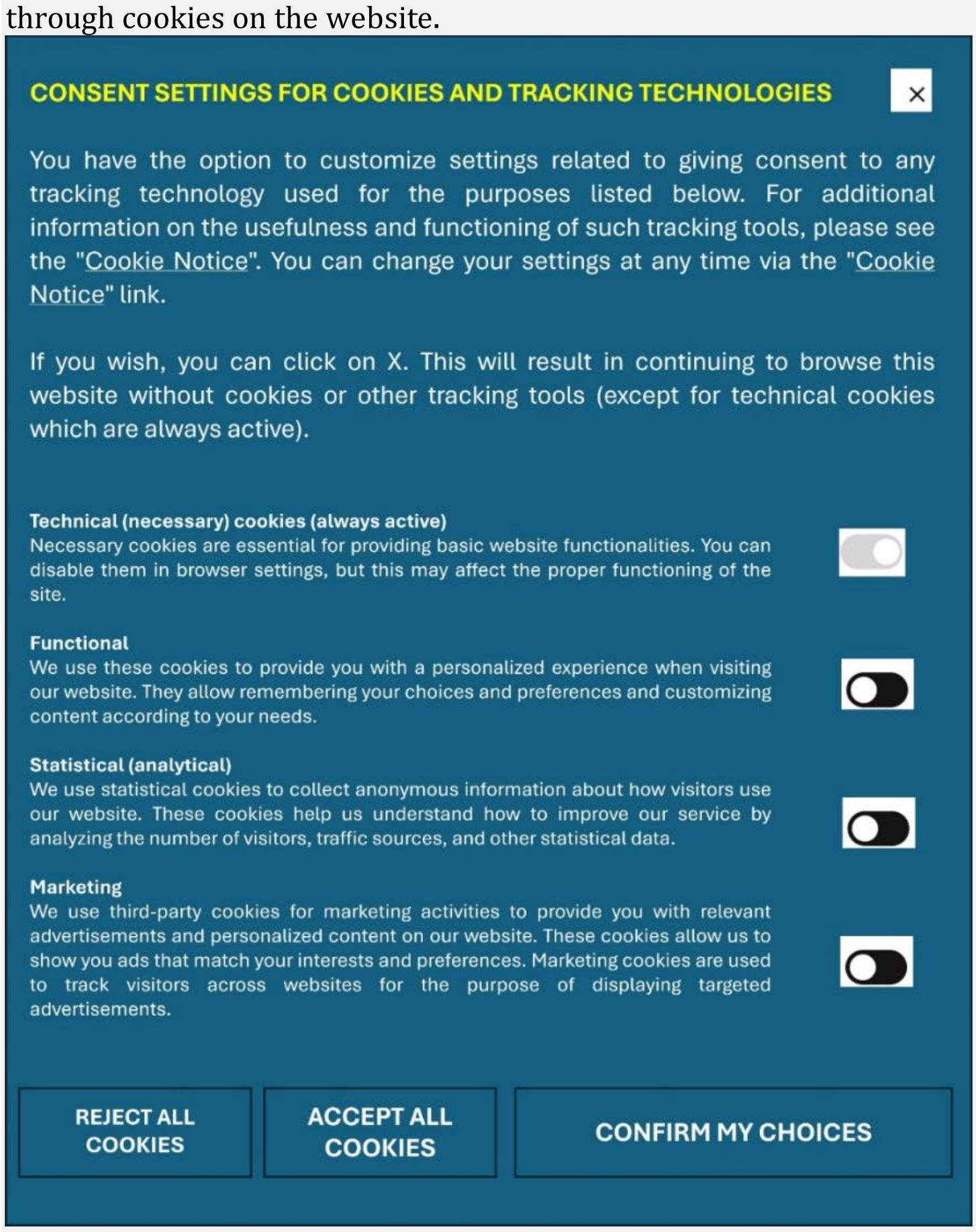
Example of good practice "Cookie Banner" (second layer)

The data subject has the option to select the types of cookies and purposes of personal data processing for which they give their consent. The initial settings are such that cookies are disabled. Through an active action, the user chooses whether they want their personal data to be processed via cookies for specific purposes. The data subject has the option to accept all cookies, reject all cookies, or confirm their selections. They also have the option to click on the X mark, after which the cookie bar closes, and the website will not process the user's personal data through cookies. The data subject also has the opportunity to learn more information about the processing of their data through cookies via the "Cookie Notice" link.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

This is an example of the second layer of a GDPR-compliant cookie consent mechanism, which provides more detailed control over cookie preferences. It emphasizes user control, transparency, and the ability to make informed choices about data processing through cookies on the website.



Notice about the processing of personal data through cookies

Regardless of how personal data is processed, the General Data Protection Regulation (GDPR) obliges the controller to inform the person from whom it directly collects and processes personal data about:

- the identity and contact details of the controller,
- the contact details of the Data Protection Officer (if required),
- the purpose of the collection/processing of personal data and the legal basis for the collection/processing,
- who has the right to consult the collected personal data,
- whether the personal data are transferred to third countries (countries outside the borders of the European Union and the European Economic Area) or international organizations,

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

- what is the retention period of personal data,
- the right of the data subject to request access to personal data, rectification, erasure or restriction of processing;
- the right to withdraw consent if consent is the legal basis for the processing,
- whether the data collected is used for automated decision-making.

This provision of the GDPR also applies to the collection and processing of personal data through cookies, regardless of whether or not cookies require consent.
Therefore, this information must be provided to visitors to the site in a conspicuous and easily accessible place.
Usually, all these data are listed on pages called, e.g. “Privacy Policy” or “Data Protection”, in which the general section contains information about the controller, the data protection officer, the rights of the data subject to request access to personal data, rectification, erasure or restriction of processing, and in a separate section related to cookies information about the types of cookies, which data are collected through cookies, for what purpose, what is the time of storage of cookies, who has the right to access certain types of cookies, whether the collected data is used for automated decision-making, the right of the data subject to withdraw the consent given for the processing of personal data through cookies.
Another option used to provide the necessary information to users is that general data about the controller, the Data Protection Officer, the rights of the data subject to request access to personal data, rectification, erasure or restriction of processing, general data on the processing of personal data through cookies are listed on pages called e.g. “Privacy Policy” or “Data Protection”, and to use a specific page for more detailed information about cookies, e.g. “Cookie Notices” or similar.
As this information should be visible and easily accessible, it is common practice to find links to it (Privacy Policy and Cookie Notice) on all pages of the website, usually in the header or footer.
It is important to note that this information should describe the actual state of the website, i.e., the actual type and categories of cookies, which personal data are actually collected by means of these cookies, what is their actual purpose and storage periods, who has the right to consult the data stored in cookies and whether the data is transferred to third countries or international organizations. Therefore, if the controller of the website is not sufficiently trained and able to analyze cookies on their website, they should do so in cooperation with the site makers and describe the actual state of their website related to cookies, and not to copy it from another website just in order to satisfy the form.
Information about cookies is also important and should always be kept up to date. Therefore, any upgrade or change of the functionality of the Internet site or any part of it that also results in changes related to cookies needs to be appropriately modified in accordance with the new condition.

Cookie law in Italy

It should be noted that cookie regulation might have some peculiarities at national level, depending on the local legislation in force and on the decisions issued by the competent Data Protection Authority.
In Italy, the applicable legislation on the matter is represented – in addition to what has been provided by the European Data Protection legislation – by art. 122 of the Italian Data Protection Code (legislative decree no. 196/2003, as supplemented by legislative decree no. 101/2018). Furthermore, in 2021, the Italian Data Protection Authority (“Garante”) issued the “Guidelines on the use of cookies and other tracking tools”

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

(available at the following link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876#english), where it is underlined the following:
Technical cookies and other technical identifiers: these are used solely for the purpose of 'carrying out the transmission of a communication over an electronic communications network, or to the extent strictly necessary for the provider of an information society service explicitly requested by the contracting party or user to provide that service' (see Section 122 (1) of the Italian Privacy Code) They do not require users' consent, however they must be referred to in the information notice/privacy policy.
First-party and third-party analytics cookies: these can be equated to technical cookies and other technical identifiers exclusively if:
- They are only used to produce aggregated statistics concerning a single site or a single mobile app;
- At least the fourth component of each IP address is masked out as for third-party cookies; and
- The third parties do not match the analytics cookies data with any other information (such as customer records or statistics concerning visits to other websites) and do not forward such data to other third parties. However, statistical analyses concerning several domains, websites or apps that can be traced back to the same publisher or group of undertakings are allowed. Where a controller produces, through its own resources, statistics on data relating to several domains, websites or apps that can be traced back to that controller, non-encrypted data may also be used providing purpose limitation constraints are complied with.
Non-technical cookies and other tracking identifiers: these are used to trace specific actions or recurring behavioral patterns in the use of the offered functionalities back to specific, identified or identifiable individuals for the purpose of grouping the different profiles within homogeneous, multi-sized clusters; this is aimed in turn to enable increasingly customized services along with the sending of targeted advertising messages, i.e., messages that are in line with the preferences expressed by users during their web-browsing activities.
Main changes under the GDPR concerning cookies and other tracking tools:
Accountability;
Expanded information obligations (data storage periods to be specified as well);
Enhanced consent (it must be 'unambiguous' in all cases);
Compliance with privacy by design and privacy by default principles.
Information and consent: information should be provided:

- by using simple, accessible language;
- in such a way as to be conveyed, without any discrimination, also to individuals needing assistive technologies or special configurations on account of their disabilities;
- also by relying on multi-layered, multi-channel approaches;
- if only technical cookies are used, the relevant information may be placed on the website's homepage and/or in the general information notice;
- if other cookies and non-technical identifiers are also used, a suitably sized pop-up banner can be used including:
- a warning to the effect that the website uses technical cookies as well as (subject to user's consent) profiling cookies or other tracking tools along with information on the relevant purposes (short information notice);
- a link to the privacy policy containing the extended information notice and mentioning any additional recipients of the personal data, data storage periods and how to exercise the rights under the GDPR;

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

- a warning to the effect that if the banner is closed (e.g. by clicking on the 'X' on its top right corner) the default settings are left unchanged and therefore browsing can continue without cookies or other tracking tools other than technical ones. Accordingly, the banner will have to contain the following in order to obtain valid consent:
- the command referred to above (e.g., an 'X' placed on the top right corner) to close the banner without giving one's consent to the use of cookies or other profiling techniques and by keeping default settings;
- a command (button) to accept all cookies or tracking tools;
- a link to an additional dedicated area where the user can select, individually, the functionalities, the third parties, and the cookies that user consents to install, and where the user can either consent to the use of all cookies (if such consent has not already been given) or withdraw his/her consent, also once and for all.

In this regard, a good practice consists in using a graphical sign, an icon or any other technical arrangement to flag (e.g. in the footer of each domain page) the status of the consent declarations given by each user, and to enable changing or updating such declarations.

This dedicated area will have to be accessible also through an additional link to be placed in the footer of each domain page. Soliciting consent repeatedly is not permitted if consent has been withheld, except where any one of the following conditions applies: one or more of the circumstances of the processing changes significantly; it is impossible for the website operator to know whether a cookie has already been stored on the device; at least six months have elapsed since the banner was last presented. Regarding authenticated users (i.e., users having registered accounts), the data relating to their browsing across several devices may not be matched except with the users' prior consent.

Assessment of methods to obtain consent: in relation to scrolling, it is per se unsuitable to obtain valid consent unless it is part of a broader process enabling a user to generate an event that can be recorded and documented in the website server and can qualify as an explicit action to unambiguously signal that user's intention to consent to the processing. With regard to the cookie wall, it is unlawful, except where the website enables a user to access equivalent contents or services without consenting to the installation and use of cookies. This will have to be assessed case by case and in the light of GDPR principles.

Validity of existing consent: pre-GDPR consent remains valid if it meets GDPR requirements and is recorded at the time it was obtained, i.e., if it can be documented.

Cookie Law in Croatia

The processing of personal data through cookies in the legislative framework of the European Union is regulated by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). These directives have been implemented in the Republic of Croatia through the Electronic Communications Act (Official Gazette 73/08, 90/11, 133/12, 80/13, 71/14, 72/17, 76/22, and 14/24).

Regarding the use of so-called cookies, in the Republic of Croatia, the Electronic Communications Act (Official Gazette No. 73/08, 90/11, 133/12, 80/13, 71/14, 72/17, 76/22, and 14/24) applies as a special law. Article 43, paragraph 4 of the cited Act

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

stipulates that the use of electronic communications networks for storing data or accessing already stored data in the terminal equipment of subscribers or service users is permitted only if the subscriber or service user has given their consent, after receiving clear and complete information in accordance with special regulations on personal data protection, particularly regarding the purposes of data processing. This cannot prevent the technical storage of data or access to data solely for the purpose of carrying out the transmission of communications via an electronic communications network, or, if necessary, for providing information society services at the explicit request of the subscriber or service user.

According to the above, the legal basis for collecting personal data using cookies (stored on the computer/terminal equipment of the end user), except in specifically stated exceptional cases, is the consent of the end user, which should be in line with the provisions of the General Data Protection Regulation, specifically Article 4, paragraph 1, point 11, which 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.

Data controllers cannot rely on legitimate interests within the meaning of Article 6, paragraph 1, point (f) of the General Data Protection Regulation as a legal basis for using electronic communications networks to store data or to access already stored data in the terminal equipment of subscribers or service users. We particularly emphasize that relying on legitimate interest for processing personal data of data subjects through cookies (storing cookies on the data subject's terminal equipment/accessing already stored data in the data subject's terminal equipment) for marketing purposes is contrary to legal regulations on personal data protection. Furthermore, in 2020, the Croatian Personal Data Protection Agency (AZOP) issued recommendations and guidelines on the processing of personal data via cookies and other tracking technologies, available at https://azop.hr/obrada-osobnih-podataka-kolacici/

Olivia can help in the managing of cookies for Croatian and Italian SMEs.

5. Rights of the Data Subject

The GDPR enshrines fundamental rights for individuals concerning their personal data. These rights are crucial not only because organizations are legally obligated to respect them but also because they empower individuals to enforce their rights when they believe an organization is infringing upon them. Notably, some of these rights are applicable irrespective of any suspicion of breach or non-compliance by a firm.

SMEs must carefully consider the various rights afforded to individual data subjects, as each right pertains to distinct issues and thus requires establishing separate procedural mechanisms. Additionally, SMEs must implement and maintain procedures, records, and documentation to demonstrate compliance with data protection regulations to supervisory authorities in case of a query, audit, or complaint (see above the accountability principle). It is essential to establish comprehensive compliance procedures and mechanisms for managing disputes to ensure that the organization is adequately prepared in the event of complaints or litigation initiated by individual or group data subjects.

VIII. Guidelines (controller and processor)

The written agreement between the controller and the processor can clarify how the processor will specifically assist the controller in fulfilling the data subject’s requests.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION’S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

In principle, the controller must respond to the data subject's request "without undue delay" and within one month (Article 12, Paragraph 3). This period may be extended by two months if necessary, provided that the data subject is informed within 30 days and the delay is "duly motivated" (e.g. due to the complexity of the issues the number of requests). Data subjects can make the request orally (e.g. by telephone) or in writing (e.g. by email, post, social media).

Not all requests from data subjects are justified. Suppose data subjects' requests are manifestly unfounded or excessive (e.g. repetitive). In that case, the controller may charge a reasonable fee based on the actual administrative costs incurred in processing the request (no penalty fee may be charged) or refuse to act. However, the controller is burdened to prove that the request is manifestly unfounded or excessive.

Before acting on a request, the controller must verify the requester's identity. This prevents third parties from gaining unlawful access to the personal data of others. In some cases, requests relating to the exercise of data subject rights may come from third parties and not directly from the data subject.

IX. Guidelines (practical example of rights' recipients)

When considering the respective rights, organizations must not overlook the potential recipients of these various data protection rights. These rights generally apply to any individuals whose personal data are being collected and processed. Specifically, the recipients of these rights may include, for instance:

- Employees.
- Other workers, such as contractors, temporary staff, and casual employees.
- Agency staff.
- Former employees and retirees.
- Job applicants, including those who were unsuccessful.
- Volunteers.
- Apprentices and trainees.
- Customers and clients.
- Prospective customers and clients.
- Users of services provided without monetary remuneration.
- Suppliers.
- Related family members.
- (…)

Olivia can help you to develop a template for data subject requests.

A. Right to transparency and information

Transparency enables organizations to design and implement lawful data processing processes and procedures. It also empowers individuals to enforce their rights and gives them confidence in data processing activities' security. Scholars have stressed the importance of transparency for "data protection", considering this as a "transparency right" that should enable individuals and others to act on their data (positive freedom) while imposing some positive obligations on those who determine the purpose of processing.

SMEs' privacy and data protection notices must comply with these requirements. The GDPR affirms a "duty" to facilitate the exercise of rights. A clear and transparent privacy and data protection notice will increase data subjects' confidence, and could very

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

likely reduce the number of queries from data subjects. For more explanation on the obligations related to these rights for SMEs see also the description of the principle of transparency.

Data subjects must be informed, in **clear and simple language**, of:

- the main elements of the processing operations (e.g., type of personal data processed, legal basis, specification of purposes, data retention period, possible data transfers, etc.);
- the contact details of the parties involved (e.g., data controllers and, if applicable, DPOs and recipients);
- the data subjects' rights and how to exercise/claim them.

Information must be provided in writing or through other appropriate means, including electronically. Upon request, information may be provided orally as long as the data subject's identity is verified through other means. Data subjects have the right to access information free of charge. Responding to requests should generally be done within one month of receiving the request.

X. Guidelines

There are several techniques that SMEs can use to provide information:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons;
- mobile and smart device functionalities;
- cartoons, infographics, or flowcharts.

B. Right to Access

Right to access means the right to be informed by the controller whether their personal data are being processed and, if so, to obtain access to and a copy of the personal data being processed. The idea behind the right of access is to enable data subjects to verify the lawfulness of a controller's data practices. When responding to a request for access, the controller must provide the data subject with the following information:

- confirm the identity of the data subject in order to determine whether personal data relating to the data subject(s) are being processed;
- provide a copy of the personal data being processed (unless this would affect the rights and freedoms of others);
- provide information on the purposes of the processing;
- the categories of personal data concerned;
- the (categories of) recipients (to whom else the data will be disclosed)
- the conservation period, i.e. how long the personal data will be or the criteria on the basis of which this is determined;
- the existence of the right to obtain from the controller the rectification, erasure, restriction of processing or objection to the processing of personal data concerning the data subject;
- data concerning the data subject;
- the existence of the right to lodge a complaint with a supervisory authority;
- the source of the personal data if they have not been obtained directly from the data subject;

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

- the existence of automated decision-making, including profiling, together with meaningful information about how such decision-making works ("the logic involved"), as well as the significance and the envisaged consequences of such processing for the data subject;
- the existence of appropriate safeguards for data transfers to third countries or international organizations.

35. Example

An insurance company client has inquired about the legal basis and purposes for which the company collects a copy of their ID card, the duration for which the ID card copies are retained, and the procedures that will be followed once the purpose for retaining the copy has expired. The insurance company is legally obligated to provide a detailed response to the client's inquiry. If the company is collecting the ID card based on a legal obligation, it must clearly specify the relevant legal provision (including the specific article of the law) and the purpose for which the ID cards are being collected. Additionally, the company must inform the client of the retention period for the ID card copies and explain what will happen to the copy once the purpose for which it was collected and stored has been fulfilled.

36. Example

A company specializing in organizing educational events has received a request from a data subject asking for a copy of their personal data. The company collects the data subject's personal information (name, address) for the purpose of entering into a contract with the data subject, and additionally collects email addresses, education information, and data on the data subject's interests in order to send them information about new educational events. The company must provide, upon the data subject's request, a copy of the contract containing their personal data and a confirmation that it collects their email address, education information, data on the data subject's interests, and a list of educational events in which the data subject has participated.

XI. Guidelines

Two of the most commonly used rights by data subjects are confirmation and access rights in relation to personal data. Organizations must comply with the new GDPR confirmation and access rights. This includes preparing policies and procedures in advance, such as designing sets of standard reply correspondence and sets of internal requests to departments, guidance, and so on.

In response to an access request, a SME must:

- Supply the information to the individual data subject promptly and within a specified number of days of receiving the request.
- Provide the information in a form that will be clear to the ordinary person; for example, any codes must be explained.

C. Right to Rectification

The data subject is entitled to obtain from the controller, without undue delay, the rectification of any inaccurate personal data concerning them. In consideration of the purposes of the processing, the data subject also has the right to have incomplete personal data completed, which may include providing a supplementary statement.

The right to rectification is helpful for data subjects and SMEs, as it facilitates the maintenance of up-to-date data. Whether the controller has disclosed the personal data

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

subject to rectification to other recipients, it is imperative to inform each recipient of the rectification unless doing so proves impossible or requires a disproportionate effort.

In most cases, rectifying personal data will simply involve contacting the data controller and requesting the necessary corrections, such as for an inaccurate email address or residential address. There are situations where the data controller may not be able to rectify the data immediately, but must first verify the inaccuracy of the personal data, particularly when such data is pertinent to legal relationships.

37. Example

An individual has taken out an insurance policy. Upon discovering that the insurance company has inaccurate information about him, listing him as a smoker with cardiovascular diseases, he realizes that this misinformation has led to a higher insurance rate being applied.
The individual has the right to contact the insurance company and request the rectification of his/her data. The controllers are obligated to rectify the data as soon as possible and no later than within one month.

D. Right to Erasure (Right to be Forgotten)

The right to erasure is a direct manifestation of the principle of minimization, which dictates that personal data should be limited to what is necessary for the purposes for which the data are processed. If the data are no longer required for the purposes of processing carried out by the controller, the controller should refrain from processing the personal data.

Data subjects have the right to erase their personal data from the controller's records.

The controller must erase personal data when:

- they are no longer necessary in relation to the purposes for which they were processed;
- they were collected in relation to the provision of information society services to children;
- they have been processed unlawfully (for example, without a legal basis);
- the data subject withdraws consent or objects to the processing and there is no other lawful basis for the processing;
- Union or national law requires the controller to do so.

There are many exceptions to the right of erasure. These may include exercising the rights of expression and information, complying with a Union or national legal obligation requiring the processing, and exercising or defending legal claims.

Where the controller has disclosed the personal data to be rectified to other recipients, he should communicate any erasure request to each recipient unless this proves impossible or involves a disproportionate effort.

38. Example

An individual initially consented to receiving direct marketing, specifically special offers from a retail company. Subsequently, the individual changed their mind and no longer wished to receive such offers, requesting to be removed from the email list. The retail company must delete the individual's email address from the list and cease sending offers.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

39. Example

An individual attended a public event where it was announced that the event would be recorded and group pictures of participants would be taken and published. After a few days, the individual's photo was posted on the event organizer's social media account in a manner that was inappropriate and could potentially harm the individual's reputation and finances. As a result, the individual exercised their right to erasure. The organizer promptly removed the photo from social media and deleted it from their database as the legitimate interests of the organizer did not outweigh the individual's rights.

40. Example

An individual no longer wishes to be a member of a gym and requests the erasure of all personal data held by the gym. The gym must delete the individual's personal data as it is no longer required for the purpose for which it was collected, namely gym membership.
It is crucial to note that the right to erasure is not absolute and has limitations. Thus, it must be balanced with other rights and interests.

E. Right to restriction of processing

Individuals have a right to restrict the processing of personal data by organizations relating to them or not to be subject to processing about them. The data subject may request the controller to temporarily restrict the processing of his or her personal data in any of the following circumstances:

- The individual data subject contests the accuracy of the personal data for a period enabling the controller to verify the accuracy of the personal data.
- The processing is unlawful, and the individual data subject opposes the erasure of the personal data and requests the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of processing, but the individual data subject requires them for the establishment, exercise, or defense of legal claims.
- The individual data subject has objected to processing* pending the verification of whether the legitimate grounds of the controller override those of the individual data subject.
- The controller must notify any restriction to any recipient to whom the personal data have been disclosed unless this proves impossible or involves a disproportionate effort (Article 19). In addition, the controller must notify the data subject before the restriction on processing is lifted.

XII. Guidelines

In some instances, apart from erasure and the right to be forgotten, an individual data subject may prefer that the processing of their personal data is confined or restricted. SMEs may enforce a right to have such restrictions apply.

41. Example

An individual suddenly starts receiving bills for services from a telecommunications company. He is unpleasantly surprised because he does not use the services of that company nor has he entered into a contract with them. After investigating, the individual discovers that someone has used his ID and misused his personal data to enter into a contract with the telecommunications company and purchase three mobile phones. The

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

individual reports this criminal offense of data misuse to the appropriate authorities (police, public prosecutor's office) and has the right to request from the controller not to process his personal data for the purposes of the contract's performance.

F. Right to data portability

Data subjects have the right to data portability in situations where personal data provided to a controller are processed by automated means on the basis of consent or where the processing of personal data is necessary for the performance of a contract and is carried out by automated means. This means that the right to data portability does not apply in situations where the processing of personal data is based on a legal basis other than consent or a contract.

At a practical level, data subjects have the right to transfer their personal data directly from one controller to another where technically feasible. To facilitate this, controllers should use interoperable data formats that allow data portability for the data subject. The formats should be machine-readable, structured, and commonly used. The GDPR does not provide recommendations on the specific format to achieve data portability. The right to data portability does not create an obligation for data controllers to adopt or maintain processing systems that are technically compatible with those of other organizations. Implementing data portability solutions may benefit SMEs in circumstances where such solutions facilitate switching between service providers.

XIII. Guidelines

Examples of suitable formats for data portability include CSV, XML, and JSON, which are structured, commonly used, and machine-readable. However, controllers are not obligated to use these formats. Other formats, such as RDF (Resource Description Framework), also meet the requirements of data portability. Controllers should ensure that individuals or other controllers can effectively use the format in which the data are delivered.
Controllers can directly transmit the requested data to the individual or provide access to an automated tool that allows the individual to extract the data themselves. In both cases, it is essential to ensure that this process is carried out securely.

42. Example

A customer of an insurance company wishes to transfer their personal data directly to another insurance company to receive a personalized offer based on the data collected by the first insurance company. Upon the individual's request, the insurance company transfers the data of its former customer to another insurance company in a structured, commonly used, and machine-readable format, allowing the individual to exercise their right to data portability.

43. Example

An individual using a music streaming service wants to switch to a different music streaming platform. They have the right to request their current music streaming provider to transfer their personal data to the new music streaming provider, including their personal playlist and preferences that impact the content offered to them, such as song recommendations based on their music preferences.
In summary, the right to data portability enables individuals to receive a copy of their personal data in a structured, commonly used, and machine-readable format. This right differs from the right to access information, as individuals can obtain a copy of their

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

personal data. When individuals exercise their right to data portability, the data must be provided in a specific format and can only be applied if the legal basis of processing is consent or contract, and if the personal data are processed by automated means.

G. Right to Object

The of the data subjects to object to processing their personal data is predicated on the assumption that individuals should be able to contest the processing of data that pertains to them. These provisions relate to processing necessary for performing a task for the purpose of public interest, exercising official authority vested in the controller or processing necessary for the legitimate interests pursued by the controller or a third party, respectively. The right to object also extends to profiling activities based on these grounds.

The exercise of this right is not unconditional; it must be grounded in the specific, particular circumstances of the data subject. This implies that the objection must be justified by reasons pertaining to the data subject's situation, thus establishing a personal connection between the objection and the data processing at issue.

Upon exercising this right, the data controller is legally obligated to cease processing the personal data in question unless the controller can demonstrate compelling legitimate grounds for the processing. These grounds must not only be legitimate but must also be sufficiently compelling to override the fundamental rights and interests of the data subject. Alternatively, the processing may continue if necessary to establish, exercise, or defend legal claims.

In this context, the burden of proof lies with the controller, who must substantiate the necessity and legitimacy of the processing despite the data subject's objection. This provision underscores the GDPR's commitment to safeguarding the rights and freedoms of individuals, emphasizing the principle that the protection of personal data is paramount unless there are overriding justifications to do the contrary.

From a practical standpoint, this right compels organizations to put in place mechanisms that make it easy for data subjects to exercise their right to object, respond promptly and diligently, be transparent and accountable in their processing activities, and maintain records of objections received and the decisions and justifications.

This documentation should be comprehensive and available for review by data protection authorities if required.

SMEs must implement technical and organizational measures to facilitate the right to object, e.g., ensuring that their data processing systems are capable of flagging and halting processing when an objection is raised (this may involve automated tools that recognize and respond to objections, especially in cases of automated profiling), and adopting data minimization principles and segmenting data processing activities. Blocking cookies on a webpage is a way to object to the processing.

XVI. Guidelines

Employees, particularly those involved in data processing or customer service, should be trained to recognize and handle objections appropriately. This includes understanding the legal basis for processing and how to apply the right to object.

44. Example

A person who frequents a beauty salon discovers that video surveillance is in place, capturing not only the entrance and cash register but also clients during beauty treatments. Feeling uncomfortable with this level of monitoring, the client objects to the

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

processing of her personal data in this manner. The beauty salon must demonstrate a compelling legitimate ground for the processing that outweighs the individual's rights. If such grounds cannot be demonstrated, the beauty salon must discontinue processing the individual's personal data via video surveillance.

H. The Right not to be Subject to a Decision Made Solely on Automated Decision-Making (and Profiling)

Organizations are increasingly relying on automation and automated decision-making processes, including profiling. **Automated decision-making** (ADM) is the ability to use technology without human intervention. Automated decisions can be based on any type of data. An example of such data could be data provided directly by the data subject by answering a questionnaire or location data collected through an application.

The growing dependence on automated decision-making, mainly done by AI, raises significant concerns, particularly when such automation leads to decisions about individuals without human oversight. One of the primary issues is the potential for adverse decisions, which may need to be corrected and made without human input or the ability to identify and rectify errors. Additionally, there is widespread concern about the impact of advanced profiling techniques on data protection, as these techniques can further exacerbate the risks associated with automated decision-making.

Profiling is any form of automated processing of personal data that involves using personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Where such decisions have legal effects or produce significant effects and thus significantly affect individuals' lives, the data subject has the right not to be exclusively subject to such automated decisions. In cases when the automated decision-making is not exclusive, the controller must implement suitable measures to safeguard the data subject's rights and legitimate interests, at least the right to obtain human intervention on the part of the controller to express their point of view and to contest the decision.

For SMEs to handle an automated decision-making process, it is essential to define the scope of the ADM, ensure transparency and communication, implement human oversight, regularly audit the system, maintain accountability and documentation, and comply with ethical and legal rules.

45. Example (and Guidelines)

A company uses an automated system to calculate the annual bonuses awarded to its employees. This system analyzes various performance metrics, such as productivity, efficiency, and adherence to targets, to generate a bonus recommendation for each employee. However, determining an employee's annual bonus has considerable implications, as it directly impacts their financial remuneration and can significantly affect their overall compensation, morale, and motivation.

Given the substantial effects that the bonus amount may have on an employee, the GDPR's final decision regarding the allocation of bonuses must not rely solely on the automated system. In accordance with principles of fairness and accountability, the results produced by the automated system must be subject to thorough human review. This review involves a human decision-maker scrutinizing the automated calculations, taking into account any additional contextual factors that the system may not fully

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

capture, such as individual circumstances, extenuating performance factors, or discrepancies in the data.

Human oversight ensures that the final decision on the bonus is not only based on quantitative data but also considers qualitative aspects that require judgment and discretion. This dual approach, i.e. combining automated efficiency with human discernment, helps mitigate the risks associated with solely automated decision-making, such as potential biases, errors, or oversights inherent in algorithmic processes. It also aligns with regulatory requirements, such as those stipulated under the GDPR, which mandate that decisions with significant effects on individuals should not be made purely by automated means without meaningful human intervention.

46. Example

An individual applied for a job on a social media platform using an application form published by the social media provider. Although the individual satisfied all the criteria on the job application, they were not invited for a job interview. The individual sought clarification about the recruitment process from the data controller (social media) and discovered that the organization used pre-programmed algorithms that were fed with inaccurate data about them, leading to an unfair outcome that placed them in a group of people who do not meet the job criteria.

I. Right to Prevent Direct Marketing Processing

Individual data subjects possess the right to object to the processing of their personal data for direct marketing purposes. When personal data are retained for direct marketing, the data subject may formally request the data controller to take one of the following actions:

- To refrain from processing the data for direct marketing purposes.
- To discontinue the processing of the data for direct marketing purposes.

Upon receiving a request to cease processing, the controller must erase the relevant data within a specified period, within the timeframe stipulated by law. If the data are used for both direct marketing and other legitimate purposes, the controller must stop processing the data specifically for direct marketing purposes while continuing to use the data for other authorised purposes.

Furthermore, the controller is required to notify the data subject in writing once the processing has ceased and, where applicable, to inform them of the other purposes for which the data may still be processed.

If personal data are processed for direct marketing purposes, the data subject must have the right to object at any time to the processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data must no longer be processed for such purposes. This has significant consequences, given that marketing is crucial for many organizations.

XV. Guidelines

Direct marketing presents many problems for the public, consumer bodies, and regulators. There are restrictions or controls on how organizations operate marketing data. In terms of data protection, the rule is that data subjects have a right to object to data protection for use in direct marketing activities.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

47. Example

An individual who regularly shops at a grocery store provides their personal data to obtain a loyalty card and consent to direct marketing purposes. Subsequently, the individual receives a high volume of advertisements and promotional materials via email. Later, the individual decides they no longer wish to receive such materials and objects to the data controller (the grocery store), requesting to stop sending promotional materials. The controller complies with the individual's request by ceasing the processing of their data for direct marketing purposes.

Olivia can help you draft the Data Processing Agreement.

6. DPO

Under the GDPR, organizations are required to designate a Data Protection Officer (DPO) to oversee compliance with data protection obligations. The DPO is designated by the controller or processor to perform support and control, advisory, training and information functions in relation to the application of the GDPR. To this end, he must be "promptly and adequately" involved in all matters concerning the protection of personal data, also with reference to interlocutory activities with the Authority (such as, for example, hearings, inspections or meetings held in various capacities). It also cooperates with the Authority and is the contact point for the latter and for data subjects on issues related to the processing of personal data .

This role is essential in ensuring that the organization adheres to the stringent requirements set forth by the regulation. The DPO's responsibilities encompass a wide range of tasks, including managing data protection compliance, handling data subject access requests, and ensuring that all data processing activities are conducted in accordance with GDPR principles.

The role and responsibilities of the DPO are now more clearly defined than ever before. The DPO, who is not required to be formally certified or enrolled in special registers, must have an in-depth knowledge of the legislation and practices on the protection of personal data, as well as of the rules and administrative procedures that characterize the specific sector of reference. He/she must be able to offer, with the degree of professionalism commensurate with the complexity of the task to be performed, the advice needed to design, verify, and maintain a personal data management system, assisting the data controller or processor in adopting a set of organizational measures (including security measures) and guarantees appropriate to the context in which he/she is called upon to operate.

The GDPR expressly provides that the DPO may be an "employee" of the controller or processor capable of performing his or her duties autonomously and independently and in direct cooperation with the organization's top management. Moreover, the DPO, to be identified in any case as a natural person, may also be supported by a special office with the necessary competencies for the performance of his duties.

Where the DPO is identified in an external person, the latter may also be a legal person, provided that the natural person is indicated as the point of contact with the data subjects and with the supervisory authority.

The GDPR provides that a business group may designate a single DPO, provided that this controller is easily "reachable" from each establishment.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

Conversely, where a single DPO is not chosen but individual DPOs are appointed for each entity within the business group, in order to ensure effective coordination of the tasks assigned to them, the opportunity of setting up a network of DPOs could be considered, identifying, where appropriate, also a reference figure (e.g. the DPO of the parent company) with functions aimed at ensuring an adequate connection between them (e.g., by means of periodic meetings; exchange of information, etc.).

In all cases, the individual entities of the group, in their capacity as data controllers or processors, remain obligated to publish the DPO's contact details and communicate them to the competent supervisory authority.

With particular reference to Italy, the Italian Data Protection Authority ("Garante"), in order to facilitate the correct enforcement of the provisions of the GDPR, issued specific guidelines and FAQs (Frequently Asked Questions) on the DPO's appointment in the public and private sector, where the Authority clarifies several aspects related to this issue in the context of public and private entities and provides an illustrative and non-exhaustive list of organizations which may be required to appoint a DPO. They are available at the following link: https://www.garanteprivacy.it/responsabile-della-protezione-dei-dati-rpd-.

Furthermore, the Garante has also adopted an online procedure for notifying DPOs' contact details (available here).

XV. Guidelines

Where a Data Protection Officer (DPO) is appointed, he or she is responsible for the following activities:

- responding to requests from data subjects;
- having a policy for handling requests for access to data, which increases the efficiency of handling such requests;
- keeping a written record of the (oral) requests received and their follow-up, which helps a company to demonstrate GDPR compliance in the event of an investigation by a data protection authority.

XVI. Guidelines

Examples of enterprises obliged to appoint a DPO: public service concessionaires (local public transport, waste collection, water service management, etc.); credit institutions; insurance companies; credit information systems; finance companies; commercial information companies; auditing companies; debt collection companies; security institutions; political parties and movements; trade unions; cafes and patronages; companies operating in the utilities sector (telecommunications, electricity or gas distribution, etc.); employment and personnel search companies; companies operating in the health care, prevention/diagnostic health sector such as private hospitals, spas, medical analysis laboratories and rehabilitation centers; call center companies; companies operating in the health care, prevention/diagnostic health sector such as private hospitals, spas, medical analysis laboratories and rehabilitation centers; labour supply and recruitment companies; companies operating in the health care, prevention/diagnostics sector such as private hospitals, spas, medical analysis laboratories and rehabilitation centers; call center companies; companies providing IT services; companies providing pay-TV services.

Examples where the designation of the DPO is not mandatory: in relation to processing operations carried out by freelancers operating on an individual basis or otherwise not processing on a large scale; condominium administrators; agents, representatives and brokers not operating on a large scale; sole proprietorships or family businesses; small and medium-sized enterprises, with reference to the processing of personal data related

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

to the day-to-day management of relations with suppliers and employees (in the latter respect, see also Recital 97 for the definition of "ancillary" activities).

7. General Provisions and General Obligations

Each data controller (along with any applicable representatives) must keep detailed records of all processing activities for which they are responsible. These records must include the following essential information:

- **Identification Details**: The name and contact information of the data controller, and if applicable, the joint controller, the controller's representative, and the data protection officer (DPO).
- **Purpose of Processing**: A clear statement of the purposes for processing personal data.
- **Categories of Data Subjects and Data**: A detailed description of the categories of data subjects and the types of personal data being processed.
- **Recipients of Data**: The categories of recipients to whom the personal data have been, or will be, disclosed. This includes both recipients within the EU and those in third countries or international organizations.
- **Data Transfers**: If applicable, a record of any transfers of personal data to third countries or international organizations. This should include identifying those countries or organizations and, where necessary, documentation of the safeguards in place to protect the data during such transfers.
- **Data Retention Periods**: Where feasible, the expected time limits for the retention and eventual erasure of the various categories of personal data.
- **Security Measures:** When possible, describe the technical and organizational security measures implemented to protect the personal data.

The records of processing activities maintained by the controller or processor must be documented in **writing**, which includes the possibility of keeping these records in electronic form. Both the controller and the processor, along with their respective representatives, where applicable, are obligated to make these records available to the relevant data protection supervisory authority upon request.

However, these obligations are **exempted for enterprises or organizations with fewer than 250 employees**. This exemption applies **unless** the processing they conduct is likely to result in a risk to the rights and freedoms of data subjects, is not occasional, or involves the processing of special categories of data, such as sensitive personal data or personal data relating to criminal convictions and offenses. If any of these conditions are met, even SMEs must comply with the complete record-keeping requirements outlined in the GDPR. This ensures that any processing activities that pose significant risks or involve sensitive information are appropriately documented and subject to oversight.

XVII. Guidelines

Record-keeping is important for a variety of reasons. However, in this instance, record-keeping is an express requirement in relation to data collection, usage, and deletion under the new data protection regime. The regime has become more specific about record-keeping obligations and the details of what the records must contain.
Each controller and, where applicable, the controller's representative must maintain a record of processing activities under its responsibility. That record must contain all of the following information:

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

- Name and contact details of the controller, joint controller (if applicable), the controller's representative, and the data protection officer.
- Purposes of the processing.
- Description of the categories of data subjects and personal data.
- Categories of recipients, including those in third countries or international organizations.
- Details of data transfers to third countries or international organizations, including identification and safeguards (if applicable).
- Envisaged time limits for erasure of data categories (where possible).
- General description of technical and organizational security measures (where possible).
- Each processor and, where applicable, the processor's representative must maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
- Name and contact details of the processor(s) and each controller represented.
- Name and contact details of the controller's or processor's representative and the data protection officer (if applicable).
- Categories of processing that are carried out for each controller.
- Details of data transfers to third countries or international organizations, including identification and safeguards (if applicable).
- General description of technical and organizational security measures (where possible).

With particular reference to Italy, the Italian Data Protection Authority ("Garante"), in order to facilitate the correct enforcement of the provisions of the GDPR, issued specific guidelines and FAQs (Frequently Asked Questions) on Records of processing activities (available at the following link: Registro delle attività di trattamento - Garante Privacy (gpdp.it)) where the Authority clarifies several aspects related to this issue and provides two relevant templates which data controllers and processors can use (see: FAQ sul registro delle attività di trattamento - Garante Privacy (gpdp.it)).

Olivia can help you with Records of processing activities

8. A Risk-Based Approach in Practice

A risk-based approach to personal data protection emphasizes that merely adhering to data protection principles is not always sufficient to safeguard the fundamental rights and freedoms of individuals. Given the myriad ways in which personal data can be processed and the inherent complexity of data processing activities, it is essential to complement compliance with these principles with thorough risk analysis and effective risk management. This approach aims to enhance the practical application of data protection principles, adapting them to specific and evolving data processing contexts.

Although the meaning of risk within the GDPR is uncertain, following the risk-based approach, data controllers and processors are required to assess and act on risks to individuals arising from personal data processing activities. This may include a series of coordinated activities to assess, control, and reduce risks.

The four basic steps of risk management in ISO 31000 are:

1. identification

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

2. analysis
3. assessment
4. treatment.

In practice, it is up to the data controller to identify appropriate and proportionate measures depending on the activity carried out. Legal/consultancy firms help develop methodologies and make them available to their clients. There are also public ones some created by EU bodies or by the International Organization for Standardization (ISO). Of course, in adapting the obligations to the nature of the risk, more attention will have to be paid above all to the specific categories of data, together with data relating to criminal convictions and offenses (Articles 9 and 10) and the way in which they are used, such as large-scale and profiling processing, and the related security measures in the case of use in the processing of new technologies (big data, IoT, AI, etc.).

Under the GDPR, SMEs are also responsible for implementing the risk-based approach. On the contrary, with reference to other regulations applicable in the digital field that adopt a risk-based approach, such as the DSA, there may be an exemption for SMEs. Specifically, the provisions of the GDPR from which the risk-based approach is detected, and which will be briefly analyzed, are mainly addressed to the data controller, except for Article 32, which also calls into question the data processor.

Responsibility of the controller

The responsibility of conducting a risk assessment falls upon the data controller.

The controller must carry out a risk analysis of all the processing of personal data that it carries out; it must develop a strategy to reduce the risks of violation of the rights and freedoms of natural persons through the preparation of adequate measures: organizational measures (internal policies and procedures) and technical measures (cybersecurity measures). The "adequacy" of the "technical and organizational measures" must be parameterized to the risk. For example, the higher the risk of the processing, the more robust the technical and organizational measures the data controller must provide.

It is necessary to document:

a) both the risk assessment carried out

b) the mitigation measures implemented.

In this sense, it is very important that the controller documents each risk assessment and is capable of demonstrating compliance.

A. Data Protection by Design and by Default

Data protection by design means that, from the treatment design stage, the controllers verify, before and during the treatment, the adequacy of the measures and guarantees identified to implement effectively.

Data protection by default refers to the choices made regarding configuration values or processing options that are respectively fixed or prescribed in a processing system (a computer application, a service, a peripheral device, or a manual processing procedure) so as to affect the amount of personal data collected, the scope of processing, the period of storage, and the accessibility.

Technical and organizational measures refer to any method or means a controller may use in processing. The term "appropriate" means that such measures must be suitable to achieve the intended purpose, i.e., they must effectively implement data protection

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

principles. Therefore, the requirement of adequacy is intimately linked to the requirement of effectiveness.

The main obligation is to provide appropriate measures and necessary guarantees that allow the effective implementation of the data protection principles and, consequently, of the rights and freedoms of data subjects by design and by default.

The EDPB recognizes the challenges that SMEs face in fully implementing data protection obligations by design and by default and provides further specific recommendations for SMEs.

XVIII. Guidelines

The following guidance can help SMEs to ensure compliance with Article 25:
1. carry out a risk assessment at an early stage:
2. start with processing small amounts of data and gradually move to larger and more complex processing;
3. seek DPbDD assurances from manufacturers and processors, such as certification and adherence to codes of conduct;
4. use trusted partners;
5. contact data protection authorities;
6. read guidance from the above authorities and the EDPB;
7. follow codes of conduct where they exist;
8. seek professional help and advice.

9. Security of Processing

Controllers and processors must implement appropriate technical and organizational measures to ensure security commensurate with the risks involved. These measures may include, but are not limited to, the following:

- **Pseudonymization and Encryption**: Applying techniques such as pseudonymization and encryption to protect personal data.
- **System and Service Security**: Ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- **Incident Recovery**: Establishing the capability to promptly restore the availability of and access to personal data in the event of a physical or technical incident.
- **Regular Testing and Evaluation**: Implementing a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to maintain the security of the processing activities.

The SMEs have to take several organizational security measures.

- The first is carrying out a risk assessment of the personal data. Such an assessment would focus on the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed. In short, the assessment would anticipate risks that a data breach could affect data subjects.
- The second is to build a culture of security awareness within the organization by participating in training activities.
- The third is to have an information security policy foreseeing each user's role and the required permission levels. Such an access control policy would define roles that may be given access to personal data and, in this way, limit access to data necessary for that role (e.g., system administrator accounts). Furthermore, such a

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

policy could be used to demonstrate the controller's responsible behavior (Article 24) and facilitate compliance with the GDPR requirements.

The DPO could play a significant role in setting organizational security measures by raising awareness, training, and regularly auditing staff handling personal data

Security measures are sometimes thought of as protecting personal data held in computers and networks. Whilst these are important, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen, or incorrectly disposed of. Therefore, Technical measures must include physical and computer or information technology (IT) security.

When considering physical security, the following elements are relevant:

- the quality of doors and locks, and the protection of the business premises by means such as alarms, security lighting, and CCTV;
- the access control to business premises as well as the supervision of visitors;
- the disposal of any paper and electronic waste; and
- the secure storage of IT equipment, particularly mobile devices.

Technical measures fall within the domain of **cybersecurity**. This complex technical area constantly evolves, with new threats and vulnerabilities emerging.

Before determining the appropriate security measures, an SME must first assess the risks of processing personal data. This involves reviewing the personal data it holds and evaluating how this information is used, considering its value, sensitivity, and confidentiality. The SME should also assess the potential damage or distress if this data were compromised.

Additional factors to consider include:

- The nature and extent of the organization’s premises and computer systems;
- The number of staff and the extent of their access to personal data; and
- Whether a third-party processor processes any personal data.

The GDPR does not prescribe specific security measures that an SME must implement. Instead, it requires controllers and processors to ensure a level of security that is “appropriate” to the risks. This appropriateness must be assessed in relation to the risks to individuals' rights and freedoms, current technological capabilities, implementation costs, and the nature, scope, context, and purpose of the processing.

This approach reflects the GDPR’s risk-based framework and acknowledges that there is no “one size fits all” solution for information security. What is deemed appropriate will vary for each controller and processor, depending on their specific circumstances, the nature of the processing activities, the risks they pose to the organization, and the rights and freedoms of data subjects. When processing special categories of data (such as health data) or data relating to minors, higher levels of security are expected and must be properly implemented and documented.

Before deciding on appropriate measures, a SME needs to assess its personal data risk. It should review the personal data held and how this information is used to assess how valuable, sensitive, or confidential it is—as well as the damage or distress that could be caused if the data were to be compromised.

Other factors to consider are:

- the nature and extent of the organization’s premises and computer systems;
- the number of staff and the extent of their access to personal data, and
- if any personal data is held or used by a processor.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION’S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

Examples of personal data breaches in cases where the company was obligated to conduct a Data Protection Impact Assessment (DPIA), but the assessment was not carried out properly.

48. Example

Disclosure of clients' personal data to another data subject due to a software error. The insurance company (data controller) utilizes software from an IT company to send many monthly reports to clients at their designated email addresses.
During the transition to an upgraded version with new features, the "code" in the software was not configured. Generated PDF reports, if they contained more than one page, were split into several parts and each part was sent to a different client. As a result of this error, approximately 90 bank clients received emails containing the personal data of 75 other insurance company clients.
The insurance company failed to test the new software solution before putting it into production.

49. Example

A company that sells books(data controller) has a business relationship with an IT company (data processor) to sell services to users. The data processor needs to establish remote access to the data controller's information system. For this access, in addition to a username and password, additional security measures such as two-factor authentication are in place to protect the information of both the data controller and data processor.
A cybercriminal gained access to the data controller's information system with stolen credentials obtained through social engineering and extracted many personal data unnoticed.
While both the data controller and the data processor have implemented some security measures, such as two-factor authentication, the breach due to social engineering suggests that their measures were insufficient to prevent unauthorized access. Both parties should take immediate steps to mitigate the damage, including notifying relevant authorities, reassessing their security protocols, and reinforcing user awareness to better protect against social engineering threats in the future.

Remember that the DPIA is not required where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)).

50. Example

1) When the nature, scope, context, and purposes of the processing are very similar to the processing for which DPIAs have been carried out. In such cases, results of a DPIA for similar processing can be used (Article 35(1)).
2) Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation, and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis (Article 35(10)).
Where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, etc. In such cases, and subject to reassessment by the competent

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with the relevant requirements.

Conducting an **impact assessment is not mandatory** for the processing of personal data if the processing operation will not result in a high risk to the rights and freedoms of individuals.

51. Example

1) Processing patient data by individual doctors;
2) Processing client data by lawyers;
3) Processing data necessary for the routine management of schools and kindergartens (e.g., registration, invoicing, catering, transportation, school trips);
4) Processing data by the human resources department if you employ fewer than 250 employees;
5) Processing data for administrative tasks related to contracts with suppliers, orders, and payments;
6) Processing data for physical access control processes in a building if it does not involve processing biometric data or other special categories of personal data;

Processing data that is necessary for compliance with the data controller's legal obligations or for the performance of a task carried out in the public interest, if a data protection impact assessment has already been conducted as part of establishing the legal basis, unless Member States consider it necessary.

The data controller is responsible for ensuring the DPIA is carried out. It may be delegated to someone else, inside or outside the organization, but the data controller is ultimately accountable. The DPIA should be driven by people with appropriate expertise and knowledge of the project in question, normally the project team.

If your organization does not possess sufficient expertise and experience internally, or if a particular project is likely to hold a very high level of risk or affect a very large number of people, you may consider bringing in external specialists to consult on or to carry out the DPIA.

XIX. Guidelines (Key elements of a successful DPIA)

Although there is no one prescribed approach to take, the following steps can guide you through the process:

1. Identifying whether a DPIA is required
2. Describing the information flows
3. Identifying data protection and related risks
4. Identifying and evaluating data protection solutions
5. Signing off and recording the DPIA outcomes
6. Integrating the DPIA outcomes back into the project plan

DPIA is an essential tool for implementing accountability, as it helps data controllers not only to comply with the requirements of the GDPR but also to demonstrate such compliance

Failure to carry out a DPIA where the processing is subject to a DPIA is required may result in an administrative fine of up to €10 million or, in the case of an undertaking,

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is the higher.

10. Data Breach (Notification, Deadline, Security, Management)

A key element of any data security policy is the ability to prevent a breach of personal data where possible and, where it nevertheless occurs, react to it on time.

The GDPR provides a comprehensive definition of a "personal data breach" in Article 4.

Breaches may concern, jointly or severally, three profiles:

- A breach of **confidentiality** is defined as the unauthorized disclosure or accidental access of personal data.
- A breach of **integrity** is defined as the unauthorized or accidental modification of personal data.
- A breach of **availability** is defined as the accidental or unauthorized loss, access, or destruction of personal data.

Under the GDPR, data breaches must be promptly reported to both the relevant data protection supervisory authority and the affected individual data subjects. It is important to note that employees may also qualify as individual data subjects.

Failure to notify individual data subjects of a breach can result in substantial harm, particularly if they remain unaware.

Data breaches and personal data incidents have become increasingly common and frequent in the contemporary landscape. National data protection supervisory authorities regard these breaches with utmost seriousness. Substantial fines are now routinely imposed on firms, including large corporations and public institutions, for failing to protect personal data adequately. Even smaller organizations are not exempt from such penalties.

Data protection supervisory authorities possess the authority to conduct audits and inspections of organizations, which may encompass evaluations of security measures and preparedness for data breaches.

As soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the data protection supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights of natural persons . Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification, and information may be provided in phases without undue further delay.

XX. Guidelines (specific for Italy)

Sending a notification to the Italian (DPA) “Garante”.
As of 1 July 2021, the notification of a personal data breach must be sent to the Garante using a special telematic procedure, made available on the Authority's online services portal, and reachable at https://servizi.gpdp.it/databreach/s/ (See: Order of 27 May 2021).
On the same page, a facsimile template is available. It is NOT to be used for notifying the Garante but is useful for previewing the contents to be communicated to the Garante.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

To simplify the requirements for data controllers, Garante has devised and made available a self-assessment tool (https://servizi.gpdp.it/databreach/s/) to identify the actions to be taken following a personal data breach resulting from a security incident.

XXI. Guidelines (specific for Croatia)

As of 25 May 2018, the notification of a personal data breach must be sent to AZOP according to the procedure described at https://azop.hr/izvjescivanje-o-povredi-osobnih-podataka/

XXII. Guidelines (personal data breach management)

In addition to notifying the DPA of a breach in accordance with Article 33, the controller must immediately contain and mitigate the breach to prevent further data loss or unauthorized access. This may involve isolating compromised systems, revoking access rights, or temporarily taking affected systems offline. The goal is to stop the breach's escalation and protect additional data.
Another important and immediate task for the controller to perform when a data breach occurs is to set up a Data Breach Executive Team. The Team should consist of people from the IT department, legal counsel, and data protection officer (if appointed).
Setting up the Team is vital for the controller to identify the type of breach that occurred and assess the risk to the rights and freedoms of the data subjects, which can become addressees of the notification if the risk is high, as indicated by Article 34.
Thus, the Team carries out a “risk assessment” based on the information provided by the firm's sector contact persons and in cooperation with them. The enterprise's top management verifies the assessment and identifies the demeanor to be maintained vis-à-vis the data subjects and the complete notification to the DPA.
A risk assessment must consider at least the following criteria:

- the type of breach (confidentiality, integrity, availability);
- the nature, particular character and volume of the personal data;
- the ease of identifying natural persons based on the breached data;
- the seriousness of the consequences for the data subjects.
- the type of data subject (e.g. minors);
- the number of individuals affected;
- any measures already taken or planned to reduce the breach's impact.

After evaluating the risk, the controller and the Team must focus on the breach's impact and consequences. A (new) Data Protection Impact Assessment (DPIA) may be necessary to further evaluate the potential consequences of the breach.
This assessment should:

- Analyze and evaluate the specific risks associated with the breach.
- Determine the likelihood and severity of harm to affected individuals.
- Identify additional measures to mitigate or prevent further harm.

Based on the impact assessment, organizations should implement appropriate remedial actions. This could include enhancing “security measures”, offering support to affected individuals (e.g., credit monitoring services), or improving internal processes to prevent future breaches. Documenting the breach, response actions taken, and decisions made throughout the process is essential to demonstrate compliance with regulatory requirements.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

Conducting a "post-incident review" after managing the breach is vital. This review should focus on what caused the breach, how effectively it was managed, and what lessons can be learned to improve future data protection strategies. Implementing these lessons can enhance an organization's overall resilience to future breaches.
Assessing the impact of a personal data breach involves also evaluating both the "immediate and long-term consequences" for affected individuals and the organization.
Factors to consider include:

- Immediate Damages: Compromised data can cause immediate financial loss, identity theft, or unauthorized access to accounts.
- Long-Term Consequences: Assess the potential for ongoing harm, such as sustained identity fraud, long-term damage to reputation, or psychological distress.
- Legal and Regulatory Consequences: Consider the potential for legal action, regulatory fines, and the broader implications for compliance with data protection laws.
- Reputational Damages: Evaluate the potential damage to the organization's reputation, which could affect customer trust, business relationships, and market position.

Organizations can mitigate harm, fulfill legal obligations, and reinforce their data security frameworks by taking these steps. Every enterprise must prepare a document with these steps to be used in case of data breach.

11. Processing of Personal Data in Working Relationships

It is of great importance that employers and workers understand their rights and responsibilities under the applicable data protection rules. Even the conclusion of an employment relationship requires knowledge of the obligations that arise for the employer and (potential) workers.

In many cases, the employer may rely on the necessity of the processing to perform the employment contract. This enables the processing of data for day-to-day activities such as payroll, pension and supplementary insurance, sick leave remittances, and other issues related to the fulfilment of contractual obligations.

Additional obligations apply to 'special categories of personal data', which cover information relating to workers' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, and sexual orientation.

The period of work consists of various stages, such as job search, job interview, signing a contract, and the employment relationship itself. Sometimes, personal data of former workers are processed.

To achieve the legality and transparency of personal data processing and provide information related to the processing of personal data, and thus the exercise of the rights of data subjects: the right to access data, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object to the processing of personal data, the controller must explain in detail what types of personal data are collected, for what purpose and on what legal basis, how the personal data is used, i.e. who uses the personal data and what personal data protection measures are taken (for example, this can be achieved by creating and publishing privacy policies).

One key step is the need to harmonize internal acts related to employment or acts related to the protection of personal data. These acts will contain elaborated procedures

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

in a comprehensive and clear manner according to which the controller is obliged to act when collecting personal data.

With regard to Italy, the Italian Data Protection Authority ("Garante") issued some dedicated guidelines on the processing of personal data in the context of public and private workplaces, where specific recommendations can be found on the matter. In particular, the Italian Data Protection Authority adopted the following guidelines:

- Guidelines for e-mail and the Internet in the workplace, available at the following link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522;
- Guidelines on the processing of personal data in the context of private workplaces, available at the following link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364939;
- Guidelines on the processing of personal data in the context of public workplaces, available at the following link: http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1417809;
- Interpretative and applicative data protection issues, available at the following link: Questioni interpretative e applicative in materia di protezione dei dati... - Garante Privacy;
- Guidance document on computer programmes and services for managing e-mail in workplaces and processing metadata, available at the following link: Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e... - Garante Privacy.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

Annex

Some Real-Life Cases of Violation of Data Protection

Case 1

A car service offers vehicle servicing. Individuals provided their telephone numbers at the car service to inform vehicle owners that the service had been completed. Subsequently, the car service decided to engage in its marketing efforts by sending various notifications for marketing purposes. They utilized a database of individuals previously receiving vehicle servicing to send these notifications. However, the individuals were not informed about this practice beforehand. Despite receiving complaints from certain individuals (data subjects), the car service sent unwanted marketing content.

Question: *Which data protection principles have been violated in this case?*
Answer: The principles of lawfulness, fairness, and transparency.

Clarification

The contact information has been processed without a legal basis. Although the car service initially relied on a legitimate interest for processing personal data to send marketing content, validated through a legitimate interest test, subsequent complaints from individuals have invalidated the legal basis for processing personal data—specifically contact information. As a result, such processing of personal data contravenes the principle of lawfulness. In this case, individuals objected to receiving marketing content on their contact phone, leading to unnecessary stress due to the car service's unfair behavior, resulting in unjustified, harmful effects on the individual. Consequently, this processing is inconsistent with the principle of fairness. Furthermore, since the car service did not provide individuals with clear, relevant, and timely information regarding the use of their contact information for marketing purposes, their lack of transparency violates the principle of transparency.

The individual's contact information was initially collected to contact them regarding the vehicle service performed, not for marketing purposes. Therefore, if data collected for one purpose are intended to be used for a different purpose, it is essential to establish the legal basis for the data processing.

Case 2

The employer, a grocery shop, installed several surveillance cameras in its six shops to safeguard people and property. The grocery shop also assessed legitimate interests to establish its legitimate interest. The cameras were installed in a manner that subjects employees to constant monitoring without informing them that the video surveillance system, aside from protecting people and property, also serves the employer's interests by monitoring employees. One of the employees lodged a complaint with the data protection supervisory authority.

Question: *Which data protection principles have been violated in this case?*
Answer: *The principles of lawfulness, fairness, and transparency.*

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

Clarification

Cameras were initially installed to safeguard property, as well as the safety and health of workers. However, they were subsequently utilized for monitoring employees (assessing work efficiency). For this secondary purpose, no legal basis has been established, rendering such processing in violation of the principle of lawfulness.

The employer utilizes personal data obtained through video surveillance for monitoring work efficiency, despite the cameras being installed for property protection and worker safety and health. This causes discomfort and stress among employees, thus contravening the principle of fairness. Furthermore, the employer failed to provide employees with clear, relevant, and timely information regarding the use of video surveillance for monitoring employees (work efficiency), leading to a lack of transparency in the processing.

The grocery shop breached the purpose limitation principle by processing personal data through video surveillance. The personal data collected via video surveillance were not exclusively used for their intended purpose or a closely related purpose.

Case 3

An incident occurred involving the online shop (data controller) selling various online products. Specifically, an attacker exploited a vulnerability on the controller's website, gaining access to the personal data of several thousand online store buyers. The compromised personal data included, among other things, the names, email addresses, home addresses, and purchase histories of customers. The controller has identified the appropriate legal basis for collecting and processing this personal data for specific, legitimate purposes. Data subjects are informed about the processing of their data through the privacy policy available on the website. These personal data are essential for the online store to conduct its business, and retention periods for the data are established. After the designated period expires, the personal data are securely deleted. The online shop maintains records of processing activities and has implemented internal policies governing personal data protection within its business operations. Although the controller was aware of the website vulnerability, the vulnerability correction was postponed due to policy, priorities, and limited financial resources.

Question: *Which data protection principles have been violated in this case?*
Answer: *Principles of integrity and confidentiality.*

Clarification

The absence of adequate security measures on the website and the failure to implement proper technical and organizational safeguards led to unauthorized access to customers' personal data, breaching the confidentiality and integrity of the said data. In this situation, the controller may be subject to severe repercussions for violating the GDPR, such as potential fines and erosion of customer trust.

The website needs to have adequate security measures and the failure to implement proper technical and organizational safeguards led to unauthorised access to customers' data, breaching the confidentiality and integrity of the data. In this situation, the controller may be subject to severe repercussions for violating the GDPR, such as potential fines and erosion of customer trust.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

Case 4

The healthcare provider mistakenly sent the PCR test results to an incorrect email address, and the results also contained inaccurate personal data. This issue came to light when the patient requested access to their COVID-19 PCR test results from the data controller. It was then discovered that the results had been sent initially to the wrong email address. Additionally, the patient noticed that the results displayed an incorrect date of birth and personal identification number.

Question: *Which data protection principles have been violated in this case?*
Answer: *The principle of accuracy*

Clarification
The PCR test results of data subjects contained inaccurate personal data, such as date of birth and personal identification number, violating Article 5, Para 1, lett. d) GDPR.

The controller breached Article 5, Para 1, lett. f) of the GDPR by mistakenly sending the results to an unauthorized third party's email address, leading to the disclosure of health data to unauthorized individuals. This breach could have been avoided by implementing appropriate protection measures. For instance, sending the findings in a secure file with a download key through an alternative communication channel would have enhanced confidentiality and integrity.

Case 5

Local newspapers published the personal health data of a minor child of an individual in a public position. The published data included information about the child's alleged illness, age, date of birth, as well as the names of his siblings. The local newspapers defended their actions by stating that the news regarding the illness of the child of a public figure was already widely known in the local community. Thus, they argued that this situation did not constitute a violation of the GDPR.

Question: *Which data protection principles have been violated in this case?*

Answer: *The principles of lawfulness, fairness, and transparency.*

Clarification
Local newspapers unlawfully published sensitive medical data without a legal basis. Even though the individual concerned is a minor related to a person in a public role, the published information did not serve the public interest.

The publication of the information was unnecessary for the public interest and was excessive and irrelevant, violating the principle of data minimization.

Case 6

The bank processes clients' data and provides typical bank account management and lending services. Currently, the bank is in the process of developing a more advanced internet and mobile banking system. To facilitate this development, the bank has engaged the services of an IT service company. As part of the testing phase for the new application, the bank has provided the IT service provider with a database containing its clients' personal data. This data was collected from the old version of the Internet and

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

mobile banking systems to provide financial services. However, the bank's clients should have been informed beforehand that their personal data would be used for software development and testing. The database, which includes information on approximately 20,000 clients, was transferred to the IT service provider on a USB stick. The testing database consists of real customer data, including first and last names, addresses, personal identification numbers (PINs), dates of birth, places of residence, account types, account traffic data, login details for the internet banking system, and transaction information. Upon completing the project, the IT service provider delivered the new application. Subsequently, the provider decided to retain the testing data for potential use in developing and testing similar applications for other clients, as it was deemed highly valuable.

Question: *Which data protection principles have been violated in this case?*

Answer: *the principles of lawfulness, transparency, and fairness*

Clarification

The controller failed to establish a valid legal basis for processing personal data for software development and testing purposes. Clients were not adequately informed in advance about the utilization of their data for such purposes.

The data was originally collected for providing financial services. Using it for software development and testing does not align with a compatible purpose for processing personal data (purpose limitation).

The Bank transferred customer data to an IT service provider via a USB stick, which was not a secure data transfer method. The Bank and the IT service provider should have a controller-processor relationship and a contract as per Article 28 of the General Data Protection Regulation. (integrity and confidentiality).

Personal data should be adequate, relevant, and limited to what is necessary for processing purposes. Testing the application with data from 20,000 clients was excessive and unnecessary (data minimization).

Case 7

Upon arrival at the apartment, the owner requests the guests' identity card or passport and photographs them. When a guest asks why the landlord is photographing the identity card, the landlord responds that it is required by law.

Question: *Which data protection principles have been violated in this case?*

Answer: *Principle of lawfulness, fairness, and transparency*

Clarification

The controller failed to establish a legal basis for processing personal data through the practice of photographing guest ID cards/passports. Given that this action is not a legal requirement for the host, the controller's actions are inconsistent with the principles of legality and fairness. Additionally, guests were not adequately informed clearly and

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

understandably about the processing of their personal data, thus contravening the principle of transparency.

Personal data should be adequate, relevant, and limited to what is necessary for the intended purposes of processing. By photographing identity cards/passports, a broader data set is processed than what is essential for registering a guest's stay, thus contravening the principle of data minimization.

Case 8

The travel agency sends marketing messages to its clients (passengers who have previously used the services of the travel agency) without clearly identifying a legal basis for this processing. Despite receiving requests from individuals to stop sending them marketing messages, the travel agency continues to process their personal data for marketing purposes.

Question: *Which data protection principles have been violated in this case?*

Answer: *Principles of lawfulness, fairness, and transparency*

Clarification

The travel agency failed to identify the proper legal basis for processing personal data for direct marketing purposes, neglected to inform data subjects about this processing, and did not provide them with the opportunity to object to the processing of their personal data. This data processing violates the principles of lawfulness, fairness, and transparency.

Case 9

To enroll in the drugstore loyalty program, the individual must provide their name, surname, email address, phone number, date of birth, and marital status. Participation in the loyalty program is contingent on providing this information. A legitimate interest justifies the processing; however the drugstore has not carry out legitimate interest assessmen. Additionally, data subjects are not informed about the specific purpose for which the drugstore requires all personal data. Furthermore, the drugstore has not established retention periods for the processing of this personal data.

Question: *Which data protection principles have been violated in this case?*

Answer: *Principles of lawfulness, fairness, and transparency*

Clarification

The drugstore failed to conduct a proportionality test to justify its legitimate interest, and it is unclear why all the mentioned data is required to enroll in the loyalty program. The data subject was not informed of their rights regarding personal data processing, the processing purposes, and other information specified in Article 13 of the GDPR, which the controller was obligated to provide.

Personal data should be adequate, relevant, and limited to what is necessary for the purposes of processing. The need to collect additional data, such as marital status, when

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

processing personal data for the loyalty program, is not justified. Therefore, such data processing violates the principle of data minimization.

Personal data should only be retained for as long as necessary for the purposes it was processed. The company did not define retention periods for personal data, and it is unclear what happens to the data when it is no longer needed. This lack of clarity violates the principle of storage limitation.

Case 10

Before leaving the company, a malicious former employee saved a database containing all clients' personal data (names, surnames, PINs, addresses, phone numbers) onto a USB stick. The company failed to implement adequate technical and organizational measures to prevent this breach of its customers' personal data.

Question: *Which data protection principles have been violated in this case?*

Answer: principles of integrity and confidentiality

Clarification

Personal data must be processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction, or damage, using suitable technical or organizational measures. The company has not implemented adequate technical and organizational measures to prevent employees from storing personal data on a USB stick and potentially misusing it. Therefore, such processing violates the principles of integrity and confidentiality.

Case 11

The marketing agency was victim to a ransomware attack. Due to the agency's lack of regular data backups, it lost access to a portion of its clients' personal databases.

Question: *Which data protection principles have been violated in this case?*

Answer: *Principle of Integrity and Confidentiality*

Clarification

Personal data must be processed in a manner that ensures its appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using suitable technical or organizational measures. The company has not implemented appropriate technical measures, such as regular backups of personal data, to ensure the integrity and confidentiality of personal data in a hacking attack, which could jeopardize access to personal data and the continuity of business operations.

Case 12

An individual wishes to book apartment accommodation. In order to proceed with the booking, the renter requests the individual to email a copy of their bank card. Upon review of the privacy policy on the apartment renter's website, no clear legal basis or

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.

purpose for this processing is evident. Additionally, copies of bank cards are to be retained indefinitely by the data controller.

Question: *Which data protection principles have been violated in this case?*

Answer: *Principle of lawfulness, fairness, and transparency.*

Clarification

The apartment renter did not establish the appropriate legal basis for the collection and processing of personal data (bank card copies) nor did they provide the data subjects with the information required by Article 13 of the GDPR. Such processing of personal data violates the principles of lawfulness, fairness, and transparency.

Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. The necessity of collecting a bank card copy for booking apartment accommodation is not clear. Therefore, such processing goes against the principle of data minimization.

Personal data should only be stored in a way that allows the identification of data subjects for as long as necessary for the purposes for which the data are processed. It does not seem necessary to retain bank card copies indefinitely, making such processing contrary to the principle of storage limitation.

Olivia can help you to understand and respect data protection principles, find out more in module on Data Protection Principles.

***

Co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union and European Commission. Neither the European Union nor the European Commission can be held responsible for them.

Co-funded by the European Union

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S CITIZENS, EQUALITY, RIGHTS AND VALUES PROGRAMME UNDER GRANT AGREEMENT № 101072630.