Chapter 6 Guidelines for implementing DPbD in the EHR system

6.1 Introductory remarks

This Chapter provides a set of guidelines for DPbD management with technical and organisational measures to be implemented in EHRs in the European Union legal framework. The GDPR and the current data protection law for data concerning health in the EU are the foundations of the comprehensive set of guidelines. The aim of this Chapter is to provide further guidance for data controllers and developers on how to comply with DPbD obligations in the EHR environment. In fact, the book, examines how an e-health system should be designed, and the data processing be carried out in a way that supports and implements data protection principles and legal requirements in order to protect personal health data.

First of all, the Chapter explains the methodology employed to formulate the guidelines. It draws upon both the theoretical analysis and the insights discussed in Chapter 2, 3 and 4 and the applied perspective on privacy engineering, standards and tools presented in Chapter 5. This Chapter then provides and discusses the guidelines for an EHR system[1906]. The set of guidelines is classified according to the different timeframes of the processing (i.e. "before the processing" and "during the processing"), and to technical and organisational requirements or goals, which take into account the criteria of Article 25 GDPR, the data protection principles, and the different data states (i.e. data at rest, data in transit, data in use). After that, the Chapter investigates some possible scenarios at the liability level in the event of inappropriate or ineffective DPbD implementation.

1906 The set of guidelines is an evolution of and improvement on the DPbD model of privacy management that was published in: Bincoletto, G. (2019). A Data Protection by Design Model for Privacy Management in Electronic Health Records. In: M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina, & A. Bourka (Eds.), Privacy Technologies and Policy, Springer International Publishing, pp. 161–181. This paper was submitted and accepted at the Annual Privacy Forum of 2019, which has been organised by ENISA and by the European Commission at the LUISS University in Rome. *See* the programme of the Conference at <2019.privacyforum.eu/programme>. Last accessed 06/10/2021.

6.2 The methodology of the set of guidelines

According to the ENISA's Report "Privacy and Data Protection by Design – from policy to engineering", a privacy by design process is the output of several steps: the identification of risks, the identification of solutions and the formulation of recommendations, and the implementation of those recommendations[1907]. The approach is characterised by an iterative and continuous process.

Even DPbD is an ongoing procedure. It is a never-ending approach. A DPbD implementation has been theoretically divided into "four steps": "gap analysis with the specific legal framework", "risk analysis", "project steering and budget planning", and "implementation"[1908]. This research tries to create a set of guidelines for DPbD implementation in EHR systems and in the EU legal framework. In particular, the legal rules are the GDPR and the data protection framework for data concerning health described above. The comparison with the US legal framework will be taken into account since it provides useful examples of organisational and technical safeguards for medical records.

The set of DPbD guidelines defines requirements and comprehensive data protection measures that may aid data controllers (and system developers) when they opt for the architectural choices and the appropriate organisational and technical measures to be implemented, including PETs and standards. So, the set identifies requirements and formulates recommendations as comprehensive guidelines for the implementation, that may be used in the "requirement phase" of a DPbD engineering approach. The main goal is to achieve compliance with the law since data protection becomes a core component of a system.

The proposed requirements and measures take into account the legal analysis of Article 25 of the GDPR and of the data protection principles and rights, the legal investigation of the data protection framework that applies to data concerning health, including the comparative insights, and the methodologies, tools and solutions described in the technical part of this book.

1907 *See* Danezis et al., *Privacy and Data Protection by design – from policy to engineering*, p. 12.

1908 Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*.

As Article 25 GDPR applies to the full life cycle of the data processing and at the time of determination of its means, the guidelines will be divided in:

- Before the processing, i.e. at the time of the determination of the means of the processing, which includes "before collection" of personal data;
- During the processing, i.e. at the time of the processing activities, which includes "collection", "use" and "deletion" of personal data;
- (After the processing, that refers to the moment where personal data are anonymised after an anonymisation process, or are deleted).

Actually, when data are anonymised, they fall out of the scope of the GDPR, including Article 25. So, the guidelines focus on the first two time periods, but some brief considerations on the third period may still be provided at the end of the discussion.

These guidelines may specify the precise timing of "collection", "use" and "deletion" where the requirement is strictly connected with these activities. When it is not, it will be indicated before or during the processing. However, all the measures should always be implemented and often reviewed to comply with the ongoing DPbD approach.

Within this categorisation, the separate dimension of technical and organisational measures of Article 25 of the GDPR will be taken into account. This distinction follows the recommendation of the Norwegian Data Protection authority to identify both "data-oriented design requirements" and "process-oriented design requirements"[1909]. In addition, the technical measures are divided among the three states of data: data at rest (recording, structuring, storage), data in use (collection, use, consultation), data in transit (transmission, making available).

As explained above, DPbD measures are aimed at demonstrating compliance with GDPR requirements[1910]. Thus, to demonstrate compliance with Article 25, each subset of guidelines assigns the related data protection principles to the various guidelines and indicates the articles of the GDPR in brackets. It has been pointed out that from an individual viewpoint "the data subject should have control over the collections, the uses, the storage and the disclosures" of his or her personal data in the EHR[1911]. So, the set of guidelines takes into account the exercise of the data subject's rights, too.

1909 *See* Chapter 5, Section 5.2.

1910 *See* Chapter 2, Section 2.4.2.

1911 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 172.

The model presented during the Annual Privacy Forum of 2019 divided the guidelines into four groups according to the actors mainly involved[1912]. One part was explicitly dedicated to the developer of the EHR system ("the technical measures") and three parts to the data controller and data processor ("the creation of the EHR", "the use of the EHR" and "the organisational and administrative measures")[1913]. The content of the first version of the model is used here as part of the set of guidelines, but the classification has changed, and the guidelines have been enhanced. The benefit of that approach was to highlight the specific and different duties of the subjects involved and the two important dimensions of the creation of the patient's profile in the EHR and the use of the collected data. However, as demonstrated in Chapter 2 in Section 2.4.1, the developer is not directly bound to Article 25[1914].

For this second version of the guidelines a different comprehensive classification is provided. Even so, it should be specified that the developer remains a pivotal player in the DPbD implementation. The data controllers, e.g. the hospital and the pharmacy, frequently outsource the development of the EHR system and its environment to a processor. In addition, under Article 32 of the GDPR the processor shall implement security measures. Therefore, the developers should participate in the technical solutions that require a technical intervention in the EHR system. The organisational and administrative measures remain tasks of the data controllers, who will be liable under Article 83 of the GDPR[1915].

It should now be specified that the measures for the EHR system are presented within several security and data protection measures applicable to data processing where data concerning health are processed on a large scale. The guidelines may be applied to the EHR system and its source systems, e.g. HIS and CIS. The aim is to provide a comprehensive set of guidelines that may be useful for a "typical EHR environment".

This category refers to the EHR system that has been described in Table 3.1, after the description of the state of the art of this technology[1916]. The EHR of patient Jane Doe can be accessed and used by multiple entities that are involved in her care: laboratory and radiology clinics, the general practitioner, the hospital, and pharmacies of the national, regional or local

1912 Bincoletto, *op. cit.*
1913 *See* Bincoletto, *op. cit.*, p. 173.
1914 The liability issues are investigated *infra*, Section 6.5.
1915 The last section of this Chapter examines the liability issue.
1916 *See* Chapter 3, Section 3.4.1.

health service. The organisation of the health service is usually established by law. There are several source systems of healthcare providers (e.g. CIS and administrative system of the laboratory) that are connected for the HIE. So, the "typical EHR system" follows the definition of ISO/TR 20514:2005(en), which includes both the technical and the organisational levels.

The next section connects the theoretical perspective on DPbD and the legal framework with the applied perspective on the EHR system and the technical tools for designing data protection, and describes the guidelines.

6.3 *Applying DPbD to an EHR system*

Before providing a detailed classification in the next section, a description of the DPbD approach for the EHR and the guidelines will be provided here in order to better explain the technical and organisational measures.

6.3.1 DPbD and the EHR system

The data controllers in the EHR environment should have knowledge of the flow of personal data in the system, of the characteristics of their data processing activities and the applicable legal requirements under EU and Member State law. It is necessary to collect the complete set of legal requirements and guidelines of authorities (DPA, governments), and of stakeholders that are relevant to the project development. It has been suggested to order these rules in terms of hierarchy and applicability[1917].

Generally, a map of the data flows is highly recommended since DPbD safeguards should be applied in the whole data management life cycle. Data controllers should also map the technical infrastructure of the envisaged or existing systems. The data controller should evaluate all the criteria of Article 25 of the GDPR: the state of the art, the costs, the contextual factors of the processing activities, and the risks to rights and freedoms posed by these activities. DPbD and security compliance budget planning should be defined proactively.

The concrete characteristics of the data processing should be evaluated according to Article 25 of the GDPR[1918]. Applying the criterion of "nature,

1917 Stevovic et al., "Enabling privacy by design in medical records sharing", p. 390.
1918 *See* Chapter 2, Section 2.4.4.

scope, context and purposes of the data processing", the preliminary questions, and resulting answers, for a "typical" EHR system are:

– *What is the personal data processing operation?* In the EHR context, there are typically several data controllers, which may or may not be joint controllers. If they are not, then each controller has its own purpose and determines the means of the processing. In a centralised context, one controller, e.g. a local health authority, delegates the processing to hospitals, clinics, or laboratories, but officially remains the only data controller[1919]. The "typical EHR environment" assumes that there are multiple data controllers. Each controller shall apply the DPbD requirement. The processing in the EHR system is typically on a large scale[1920]. Healthcare providers collect personal data about an individual, store them in their CDR or another internal repository that is connected to the EHR storage system (i.e. registry component), and use them through HIS, CIS or other internal systems. The integrated view of patient's data, the order entry and access to multiple knowledge resources are the functions of the EHR that allow the processing activities. This system has an interface that allows entry and query of patient's data. The source systems should be interoperable[1921]. Healthcare providers transmit data through the HIE in the local or national EHR environment. If the EHR is interoperable across Member States, personal data can be exchanged in the eHDSI between a country of origin and a country of treatment. Personal data in the EHR may be disclosed to other specified recipients under Member State law (e.g. to public authorities).
– *What are the types of personal data processed?* Both common personal data, namely contact details, administrative data, billing data, and data concerning health, including medical history, diagnoses, clinical notes, parameters and vital signs, prescriptions, radiology images and laboratory results. EHR and its source systems should be comprehensive enough to provide a useful overview of patient's health.
– *What is the purpose of the processing?* The purpose is primarily providing medical treatment or healthcare and healthcare-related services, and payment services. However, Member State law may allow other

1919 On the roles in the processing *see* Chapter 3, Section 3.4.2.
1920 However, in the case of PHR the processing may not be on a large scale.
1921 As mentioned in Chapter 5, Section 5.5, the XDS Cross Enterprise Document Sharing is a standard for managing the sharing of documents between healthcare providers.

purposes, including scientific research in the medical field, statistical research, public interest in public health, and governance purposes of the organisations.

- *What are the means used for the processing of personal data?* The means are clinical and medical ICT systems. In the EHR environment automated means are not commonly used for healthcare purposes, unless other e-health technologies are connected to the EHR. Automated means are used during scientific research activities (e.g. for mapping health threats in the population, or for genetic research). When automated means are used, Article 22 of the GDPR applies and explicit consent is required for that purpose.
- *Where does the processing of personal data take place?* The EHR environment is defined under national, regional or local law. In general, processing activities operate at the local level in a Member State. In a cross-border interoperability scenario, processing operates across two Member States.
- *What are the categories of data subjects?* Both children and adults who are patients.
- *Who are the recipients of the data?* In the EHR environment, treating physicians, nurses, professionals, and their staff use personal data. The collected data may be also used by the workforce and staff, and the administrative and accounting services. Outside the EHR environment, personal data may be shared with other specific recipients under Member State law for defined and limited purposes (e.g. public health).

As regards the evaluation of the risks, the assessment should identify threats, and estimate the likelihood and severity of possible hazards[1922]. According to the fairness principle of Article 5(a) of the GDPR, data controllers should evaluate whether the processing activities have an impact on rights and freedoms, whether it may discriminate individuals, whether the processing involves vulnerable natural persons, or creates power imbalances. Data controllers should also identify other risks posed by processing operations. In the context of ICTs and HITs common security threats are unauthorised access and disclosure of personal data, unauthorised alteration of personal data, unauthorised deletion or loss of personal data, malicious intent (e.g. hackers), interception of communications, man in the middle, malware, ransomware, identity theft, or social engineering.

1922 *See* Chapter 5, Section 5.4. The LIDDUN threat trees or the CNIL tools may be used.

For the processing operations of the use case, the impact to rights and freedoms from loss of confidentiality, integrity and availability of the EHR system or its source systems may be considered high, since the data subject may encounter significant inconveniences by the unauthorised disclosure or modification of data concerning health[1923]. The system is interconnected to several systems, the processing is performed by a large number of staff members and on a large scale, and the e-health sector is frequently prone to attacks. So, the likelihood should be considered as high-level. Accidental loss, destruction or damage and unlawful use of data concerning health in the EHR impinge on the right to respect for private and family life, the right to data protection, and potentially other rights and freedoms of the Charter of Fundamental Rights. Actually, wrong or incomplete data concerning health may put the data subject's health and life in danger. As argued above, significant economic, psychological and social harm may be caused by the hazards mentioned[1924]. Even the severity should be considered at high-level. Hence, high-level likelihood combined with high-level severity results in a high risk level[1925].

Following the evaluation of the risk level in light of the concrete data processing operations, the DPbD solutions should balance and take into account the state of the art of the technologies and of the organisational practices, and the costs of implementing the measures[1926]. Thus, the controllers should choose the measures that are available in the market and that are the most effective among them in achieving the legal protection[1927]. According to ENISA, "the most recent stage of technological development" or "the stage that incorporates the newest possible features and functionalities" satisfies the concept of state of the art[1928]. Among the

1923 In a specific use case on health service provision, ENISA evaluated the risk of a small clinic that provided health services within an electronic medical record. The authority considered the impact from loss of confidentiality, integrity and availability as high. *See* European Union Agency for Network & Information Security, *Handbook on Security of Personal Data Processing*, pp. 39–41. In the same handbook other use cases on e-health technologies (e.g. remote monitoring) ended with high risk levels.

1924 On the concerns of e-health technologies *see* Chapter 3, Section 3.2.

1925 *See* Chapter 5, Section 5.4.

1926 Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 172.

1927 *See* Chapter 2, Section 2.4.3.

1928 Guasconi et al., *Reinforcing trust and security in the area of electronic communications and online services. Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*.

technologies, the controller could choose PETs, privacy design patterns, and a specific privacy engineering methodology (e.g. PRIPARE).

At the same time, the data controller can estimate the costs and choose the measures that are feasible and affordable for their organisation. In sum, a cost-benefit analysis (i.e. subjective analysis) goes in parallel with the study of the existing solutions provided by the market (i.e. objective analysis).

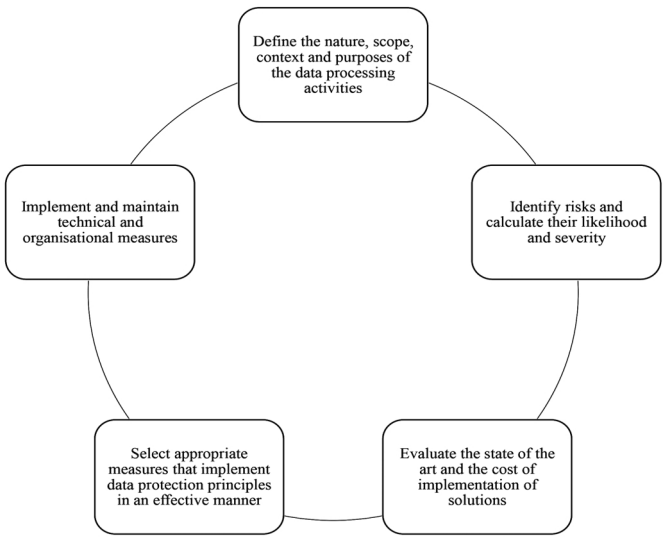
In addition to taking into account the criteria of Article 25, it is worth remembering that two adjectives are used in the provision. The appropriate technical and organisational measures shall implement data protection principles in an effective manner. The discretion with regard to the "appropriate" and "effective" criteria remains a subjective evaluation of the data controllers, who can proactively define metrics and key performance indicators[1929]. This evaluation may be later subject to scrutiny by a DPA or a court[1930].

1929 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 7, point 16.

1930 For all these considerations *see* Chapter 2, Section 2.4.6 and *infra* Section 6.5.

So, the abstract ongoing procedure of DPbD implementation may be visualised as in the following Figure 6.1.

Fig. 6.1 DPbD cycle overview



6.3.2 Technical guidelines and measures

The implementation of effective technical measures for the EHR is the first sub-set of guidelines to be dealt with. The key data protection principles are integrity and confidentiality (i.e. security) and accountability (Article 5(f), Article 32 GDPR). Nonetheless, even other data protection principles should be taken into account in the technical design stage before and during the processing activities.

As discussed in the previous Chapter, international standards and privacy engineering methodologies may play an important role in developing a secure system, and adopting these solutions may even help data controllers prove and certify legal compliance[1931]. In particular, HL7 and ISO standards on EHR may be used to ensure interoperability and a systematic

1931 The standards are indicated in Chapter 5, Section 5.5.

architecture[1932]. In addition, the EHR system should ensure the interoperability between the source systems, the vocabulary, and data formats even if they are developed by different providers.

As regards the data at rest, limits should be set on data storage before processing[1933]. Some strategies should apply to the database management system[1934]. In the EHR data controllers store both administrative/billing data and data concerning health. It has been pointed out that when administrative data reveal information on the health status of the data subject (e.g. the type of medical visit or scheduled tests) they should be considered sensitive. Removing the correlation between purely administrative data and sensitive data (e.g. during payment and administrative services) protects the confidentiality of data concerning health. So, administrative personal data could be separated from sensitive data through the separation of databases during the EHR development and in the source systems[1935]. The separation may be even operated at repository level. In addition, some data concerning health have been defined as particularly sensitive[1936]. Therefore, these data – whose types have been identified in an organisational policy – could be stored in separate modules with strict conditions for access.

1932 Above all, *see* ISO 18308:2011, ISO/HL7 21731:2014, ISO 27799:2016, ISO 13606:2019.

1933 For the following considerations *see* also Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", pp. 173–175.

1934 The following guideline also applies the "separate" strategy of Hoepman. *See* Hoepman, "Privacy Design Strategies (The Little Blue Book)".

1935 In Article 29 Working Party, Police, and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, p. 14, Article 29 Working Party argues that "patient names and other personal identifiers maintained in hospitals' information systems should be separated from data on the health status and medical treatments. They should be combined only in so far as it is necessary for medical or other reasonable purposes in a secure environment". The separation of data concerning health and demographic data is also a feature of the openEHR framework. *See* Gonçalves-Ferreira et al., "OpenEHR and general data protection regulation: evaluation of principles and requirements". *See* also Carro, Masato, and Parla, *La privacy nella sanità*, p. 69; Mehndiratta, Sachdeva, and Kulshrestha, "A model of privacy and security for electronic health records", p. 210.

1936 *See* Chapter 3, Section 3.3.1 and 3.4.2.

Encryption could be used for EHR storage to enhance the protection of data concerning health[1937]. This measure should be carefully evaluated by the controller since encryption may be used on specific files or on the full storage through software or hardware, and it affects the internal accessibility and availability of the systems. However, a robust encryption algorithm should protect the EHR server to ensure data integrity and confidentiality.

Implementing back-up and recovery mechanisms is necessary to secure the integrity of the content of the EHR and the source systems. In light of the importance of data concerning health for an individual's care, personal data should be backed up at least daily, and a complete back up of the system should be performed at least monthly[1938]. These backups should be encrypted and protected with physical security measures.

Moreover, the EHR system and its data at rest should be protected with intrusion controls and prevention systems against external attacks. Details of incidents and data breaches should be recorded. Firewalls and antivirus protection are common software security measures[1939].

The implementation of audit and log systems is a key strategy since they can track user activity in the system. This is relevant for the EHR system and the source systems because at a later stage it tracks misuse and unlawful use in a complex environment[1940]. Collecting ID number, date

---

1937 According to HIPAA encryption is an addressable measure in software and hardware for data at rest and in transit. *See* 45 C.F.R. § 170.315(d)(7) and Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 223. The CNIL recommended encryption for the storage of the French medical record. *See* Commission Nationale de l'Informatique et des Libertés, *Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux*, p. 12.

1938 *See* Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 338. The CNIL recommended regular back-ups in Commission Nationale de l'Informatique et des Libertés, *Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux*, p. 12.

1939 It should be specified that security measures should be implemented even beyond the EHR system. As an example, the workstation should be secured. Antivirus and malware protection are typical security measures. Typical physical security is equally important. Personal data should not be transferable from the workstation to external storage devices. *See* European Union Agency for Network & Information Security, *Handbook on Security of Personal Data Processing*, p. 66; Commission Nationale de l'Informatique et des Libertés, *Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux*, pp. 9- 10.

1940 This measure is also recommended in the HIPAA's requirements at 45 C.F.R. § 170.315(d)(10).

and hour, type of operation and reason for access of an event in the EHR allows the precise identification of the user and the potential source of an internal unlawful processing activity of data in use. Thus, any activity on record, including consultation, transmission, and modification, should be tracked and any discrepancies must be reported and signalled by alerts through an anomaly detection tool and an automated monitoring system. The log files should refer both to accesses to the EHR databases and accesses to the software or application. A logging level should be set before processing to include specific events and exclude useless ones since log files should be limited in size to be successfully archived and monitored[1941]. During the data use, log files should be backed up and retained securely for a certain period of time to protect their integrity[1942]. It has been pointed out that logging, reporting and auditing are evidence and tactics for demonstrating compliance and accountability[1943]. The patient may even ask to have access to the log files to learn who accessed their personal data.

During processing, all these measures should be checked and, if needed, updated frequently (Art. 24 GDPR) according to the state of the art and the cost of implementation. Both hardware and software resources should be reviewed and updated. Back-ups should be performed, and penetration tests should be carried out periodically.

Data in use should be secured[1944]. The implementation of appropriate measures for the identification, authentication and authorisation of users of the EHR systems and source systems (the workforce, staff and healthcare professionals) are fundamental for the principles of fairness, integrity, confidentiality and transparency. Identification refers to the process "to determine who the user is", authentication "to prove who a user is" and authorisation relates "to what a user can do in the system"[1945].

1941 *See* Guasconi et al., *Reinforcing trust and security in the area of electronic communications and online services. Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*, pp. 34–35.

1942 *See* Guasconi et al., *op. cit.*, p. 35, which suggests hashing and digitally signing the log files.

1943 *See* Colesky, Hoepman, and Hillen, "A critical analysis of privacy design strategies".

1944 *See* also Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 176.

1945 On access control *see* Chapter 22 of Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*. It applies to HIPAA, but as argued above the measures are useful for the DPbD implementation in electronic medical records such as the EHR and its source systems.

Thus, to ensure security of the EHR system and source systems, a system and application access and identity control should be implemented[1946]. The data controller should also implement multiple modules of presentation for the personal data at the interface level in order to differentiate between common personal data, data concerning health, and particularly sensitive data, access to which will be subject to additional authorisation.

The subjects who have concrete access to the EHR system and source systems are healthcare professionals providing treatment, administration officers and other staff. Access to personal data should be restricted to authorised subjects only, and this authorisation should be given temporarily to the subjects involved in the patient's care[1947]. Among these subjects access should be limited to specific categories of healthcare professionals[1948]. Access should be based on the role in the patient's care (nurse vs. physician) by creating different access privileges and query privileges, and a reason for the access should be contextually specified in the record. User role management should be automated, and access should be set as modular or granular. Automatic log-off should be defined[1949]. An emergency access privilege should also be implemented to protect the vital interest of the patient. Level and access rights and privileges should be reviewed regularly. Remote access (e.g. from home) should be granted sparingly. Data controllers should define specific access control strategies, such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC)[1950].

The identity verification and authentication of users accessing the EHR system and source systems should be robust. It may be advisable to use digital signature, ID badges, or smart cards that should be added to usernames and passwords. Something that is possessed by the user, such as a token, should be added to something known by the user, such as their password.

1946 Even in the US according to the HIPAA security Rule, an access control should be implemented. *See* 45 C.F.R § 170.315(d), and Thompson, *Building a HIPAA-Compliant Cybersecurity Program*, p. 155. Identity and access management is recommended for HITs by European Union Agency for Network & Information Security, *ICT security certification opportunities in the healthcare sector*, p. 18.

1947 This guideline also applies the "hide" strategy of Hoepman. *See* Hoepman, "Privacy Design Strategies (The Little Blue Book)".

1948 On these aspects it is useful to remember the case held by the Portuguese Data Protection Authority (CNPD) against a public hospital in 2018 reported in Chapter 3, Section 3.4.2.

1949 This measure is also recommended by the HIPAA's requirements at 45 C.F.R. § 170.315(d).

1950 *See* Chapter 5, Section 5.5.

Actually, multi-factor authentication is highly recommended by ENISA and by the HIPAA as an authentication method to confirm identity[1951]. For example, to access the system the user should use both username and password, and a token or a biometric mechanism[1952]. The user ID should be unique (not common authentication), and the password should be complex and have at least eight characters and it should be changed every six months[1953]. As an example, even for trainee professionals there should be a temporary and distinct authentication.

Data in use could also be pseudonymised[1954]. According to data minimisation, personal data are processed only insofar as they are adequate, relevant, and limited to the amount necessary for the purposes for which they are processed. So, state of the art pseudonymisation techniques could be applied to data concerning health[1955].

The interface of the EHR system and the source systems should automatically prompt the user to obtain patient consent or define a legal ground to prove the lawfulness of the processing[1956]. Data controllers

---

1951 *See* Guasconi et al., *Reinforcing trust and security in the area of electronic communications and online services. Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*, p. 19. *See* 45 C.F.R. § 170.315(d)(13).

1952 In order to minimise the processing of sensitive data of the workforce, a token may be preferable to biometric techniques.

1953 Obviously, passwords should not be written on a post-it note on the desk, but they should be stored in a secure way (e.g. in hashed form). They should be created with lower-case and upper-case and a combination of alphanumeric and special characters. The workstation should be automatically logged off after a certain period of time. *See* e.g. Guasconi et al., *Reinforcing trust and security in the area of electronic communications and online services. Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*, pp. 21–23; Commission Nationale de l'Informatique et des Libertés, *The CNIL's Guide on Security of personal data*, pp. 7, 11.

1954 This guideline also applies the "minimise" strategy of Hoepman. *See* Hoepman, "Privacy Design Strategies (The Little Blue Book)".

1955 On pseudonymisation techniques for health data *see* e.g. the PEP project, which provides polymorphic encryption and pseudonymisation for personalised healthcare in a research environment, in Eric R. Verheul et al. "Polymorphic Encryption and Pseudonymisation for Personalised Healthcare." In: *IACR Cryptol. ePrint Arch.* (2016), pp. 1–60. The project was referenced by ENISA as an advanced cryptography-based pseudonymisation solution in European Union Agency for Network & Information Security, *Recommendations on shaping technology according to GDPR provision. An overview on data pseudonymisation*, pp. 27–28.

1956 As an example, the legal ground could be indicated with an icon in the interface.

should also implement an automatic alert system that notifies when the legal basis ceases to apply[1957]. However, this function is not necessary when the "healthcare exception" applies, but when the legal ground is the consent of the data subject and when this consent is necessary to control the access rights of the categories of healthcare professionals[1958]. The Member State may provide more guidance on this aspect by defining the legal grounds for the EHR by law. As previously mentioned, the standard ISO/TS 17975:2015(en) provides an informational consent framework for healthcare organisations that have to obtain consent[1959]. Alternatively, a consent and choice mechanism should be implemented to facilitate obtaining consent. Data controllers should record patient's consent in a machine-readable form[1960].

During the processing, the EHR system should provide the processes to exercise the rights of the data subjects. In fact, the patient should be able control the processing in accordance with the right to self-determination. The requests of the data subject may be processed in the EHR system and source system directly. The data subject should be able to access personal data collected in the EHR by electronic means and obtain a copy. So, either the data subject should receive credentials for accessing the data or the data should be sent to the data subject. In this last scenario, the e-mail message service should be secured with encryption. It is important to remember that a medical explanation might be required for access[1961].

Where applicable, other requests to be processed are: request for concealment, request to update inaccurate data, and request for data portabili-

---

1957 If the legal basis is the vital interest, after the first medical treatment to save the patient's life, the controller shall obtain consent when required by law or use the "healthcare exception". If the legal basis is consent, when the data subject withdraws their consent, the system should alert the data controller and another legal ground should be indicated, or the system should be stopped for that individual. When the data subject is a child, and consent is given by the holder of parental responsibility over him or her at the moment the child becomes an adult, it is mandatory to collect a new consent. Meanwhile, the system should be stopped for that patient. *See* Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", p. 176.

1958 *See* Chapter 3, Section 3.4.2.

1959 ISO/TS. *ISO/TS 17975:2015(en) Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information*. Tech. rep. ISO/TS, 2015.

1960 *See* Chapter 5, Section 5.5.

1961 *See* Chapter 3, Section 3.4.2.

ty and automated decision making. In particular, the right to concealment is granted at the Member State level to conceal particularly sensitive data that concerns health (e.g. HIV disease). Technical mechanisms for concealment should be established. The right to rectification mainly concerns common personal data. The versioning of the patient's EHR should always be retained for proofing purposes[1962]. The right to data portability does not apply to public entities (e.g. hospitals) and it applies only to personal data provided by the data subject. However, the portability of data concerning health in a structured, common and automatic format empowers the data subject and so the patient may easily seek healthcare services elsewhere. The right to not be subject to a decision based solely on automated means is applicable in the e-health context, but in a typical EHR environment automated processing is not used for the main purpose of providing healthcare. It may be used for secondary research purposes. When this happens, the right may apply[1963].

As regards data in transit, the implementation of a firewall in the infrastructure can better protect the EHR network and the network of the source systems[1964]. A secure communication channel, a web application firewall, VPN, and HL7 standards are recommended. It has also been suggested to encrypt the communication channel of the EHR through cryptographic protocols[1965].

Finally, the system should ensure interoperability to allow the transfer and portability of data concerning health[1966]. To ensure interoperability

---

1962 As an example, the openEHR framework provides versioning of the data repository with digital signatures. Data is not deleted, but a new version is created. *See* Gonçalves-Ferreira et al., "OpenEHR and general data protection regulation: evaluation of principles and requirements".

1963 *See* further in Chapter 3, Section 3.4.2.

1964 *See* Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, pp. 340–342.

1965 *See* Fatemeh Rezaeibagha, Khin Than Win, and Willy Susilo. "A systematic literature review on security and privacy of electronic health record systems: technical perspectives". In: *Health Information Management Journal* 44.3 (2015), pp. 23–38, p. 29; Thompson, *Building a HIPAA-Compliant Cybersecurity Program*, p. 156; Carro, Masato, and Parla, *La privacy nella sanità*, p. 69. It is also recommended by the HIPAA. *See* 45 C.F.R. § 170.315(d)(9). *See* the guidelines on protecting the internal network of a system in Commission Nationale de l'Informatique et des Libertés, *The CNIL's Guide on Security of personal data*, pp. 13–15.

1966 In this sense, the openEHR project seems to be a good model. *See* Gonçalves-Ferreira et al., "OpenEHR and general data protection regulation: evaluation of principles and requirements".

across Member States, when provided by national law, data controllers should implement the existing tools provided by the eHDSI and the EC's exchange format tools on the patient summary, laboratory results, medical imaging and reports, and hospital discharge reports, which are usually collected in the EHR system[1967].

6.3.3 Organisational guidelines and measures

The data controller should implement appropriate and effective organisational measures[1968]. They refer to policies and procedures to be created at the management level of the data processing. As stated above, a gap analysis on the rules on data protection and health law at the Member State and local level is always recommended since the policies and procedures should be consistent with them (Art. 9(4) GDPR)[1969]. The data controller should monitor any progress and changes in the rules and update the organisational measures accordingly. At the administrative level, the risk analysis and risk management assessment are fundamental. Lawfulness, transparency, purpose limitation, data minimisation, storage limitation, and accuracy principles play a crucial role in this part (Art. 5(a) – (f) GDPR).

As regards the organisational requirements and goals before processing, the first strategy should be determining whether subjects fall under the scope of the GDPR, and under which status (Artt. 2 and 3 GDPR)[1970]. As previously mentioned, in the EHR environment there might be different controllers and processors. In the presence of joint controllers, a specific agreement should define the respective responsibilities and roles (Art. 26 GDPR). The controller should authorise the processor for the delegated ac-

1967 *See* Chapter 3, Section 3.4.3.

1968 For the following considerations *see* also Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", pp. 175–178.

1969 As an example, in the PRIPARE methodology the legal assessment should be performed through "the identification of the relevant privacy principles according to the legal framework" and "the identification of legal requirements that the system will have to comply with in order to be legally compliant, taking into account the information flows and potential risks", including soft laws such as opinions of the DPAs. *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, pp. 29–30.

1970 *See* Chapter 2, Section 2.4.1.

tivities in written form (Art. 28 GDPR). To define the concrete role of the delegated processing activities, the controller and processor should stipulate a contract or another legal act. At the same time, the controller and processor could delegate processing activities to third parties as defined by the GDPR[1971]. All the delegated activities should be regularly audited to check for compliance[1972].

A DPIA should be carried out as an organisational measure and preliminary step of the DPbD approach (Art. 35 GDPR)[1973]. The identification of risks and evaluation of solutions to be adopted should be documented since the data controller may be asked to explain why a particular measure should have mitigated a specific risk[1974]. Where required by Member State law, a prior consultation with the DPA should also be performed (Art. 36 GDPR).

The data controllers should identify a DPO, who may or may not be the same person for several data controllers in the EHR environment (Art. 37 GDPR). The DPO should be involved from the initial stages of the DPbD implementation to evaluate all aspects of compliance. This officer should monitor compliance with the GDPR and be in a position of authority within the internal management of the controller. The DPO should remain independent and objective (Art. 38 GDPR). In light of the officer's tasks, this officer could map all possible disclosure of personal data required by law (e.g. law enforcement, governance purposes of the healthcare service, public health purposes)[1975]. Policy and procedures may be set to organise possible disclosures and to limit shared personal data[1976]. In fact, when specific data concerning health shall be shared outside the

1971 *See* Chapter 2, Section 2.4.1.

1972 As an example, Carro, Masato, and Parla, *La privacy nella sanità*, p. 70 suggested the following steps: planning the audit; analysing all the documentation; interviewing the subjects involved (e.g. processor and DPO); collecting the evidence from the system and from the people; analysing the results, reporting them and finding solutions and procedures to improve compliance.

1973 *See* Chapter 5, Section 5.4. *See* also Chapter 2, Section 2.5.2.

1974 In this sense the CNIL's templates or visualisation of the measures that address specific risks are useful tools.

1975 In the PRIPARE project, the sentence "describe any disclosure, access to or transference of personal data that may be allowed" is included in the guidelines of openness, transparency and notice principles. *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, p. 125.

1976 By comparison, the identification of all possible uses and disclosures is typical in the HIPAA context. *See* Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 133.

EHR environment due to legal obligations, this disclosure does not mean that the entire data of the EHR shall be transmitted to the public recipient, but only the limited data necessary for that purpose[1977].

Creating and maintaining data protection materials and documents and conducting data protection training for the workforce and staff are other important guidelines for the accountability principle[1978]. The documentation is important since the data controller should provide evidence that the processing is data protection-compliant. The recommended policies are: privacy policy (Artt. 13 and 14 GDPR), policy on accuracy, data retention policy, policy on communication, notification and cooperation with the DPA (Artt. 31, 33 and 34 GDPR), and the policies for handling data subject requests and rights.

In more detail, the information in the privacy policy should be provided in a transparent and easily accessible form, using clear and plain language (Art. 12 GDPR). Since the data subject as a patient receives several other forms of documentation, including information on treatment and the consent form for treatment purposes, a clear and engaging privacy policy text should be drafted. In this respect, privacy icons and multiple modules could be very useful[1979]. As regards the information on the data subjects' rights, the privacy policy should be precise on the limits in the healthcare context with regard to the right to erasure and the right to data portability[1980]. At the same time, the method for exercising the right to access data

---

1977 The PRIPARE guidelines on data minimisation specify that the data controller should: "limit the purpose of personal data shared with third parties: when personal data is externally shared with third parties, share it only for those purposes identified in the privacy notice (or the legal framework authorizing the sharing) and consented by the user, or for purposes which are compatible with them; when any new personal data is proposed to be shared with third parties, evaluate whether the sharing is authorized and whether the privacy notice needs to be expanded". *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, p. 124.

1978 In this sense, HIPAA rules are good examples of establishing binding periodical training and even sanctions where covered entities are not compliant. *See* Chapter 4, Section 4.4.3.

1979 This guideline also applies the "inform" strategy of Hoepman and its architectural tactic of "explain". *See* Colesky, Hoepman, and Hillen, "A critical analysis of privacy design strategies", p. 37. On the icons *see* Rossi and Palmirani, "What's in an Icon?".

1980 *See* Chapter 3, Section 3.4.2. Taking into account when the exercise of rights is not admitted is also an insight of the HIPAA Privacy Rule that defines the limits of the rights and how the covered entity can handle the request and deny it. *See* Chapter 4, Section 4.4.2.

concerning health could be indicated in the privacy policy to facilitate the exercise of this pivotal right. Considering that the EHR could be interoperable across Member States, and that the right to receive healthcare treatment is granted in every Member State, translations of the privacy policy in at least English, French and German should be provided[1981].

The policy on accuracy ensures the quality of the personal data collected[1982]. The accuracy of data concerning health should be reviewed regularly, also to protect the health of the patient and ensure an efficient healthcare service. Since data concerning health usually are retained for a long period, an internal data retention policy could define the types of information and the respective storage timeline (provided by law frequently[1983]). The policies on communication, notification and cooperation with the DPA should identify the procedures for these activities (Art. 31 GDPR). Templates and forms could be arranged before the start of processing.

A record of the processing activities should be created and maintained (Art. 30 GDPR). Examples of records are frequently provided by the national DPAs[1984].

The workforce and internal staff, both medical and non-medical professionals, should participate in a course on data protection and security and administrative staff should be specifically bound by confidentiality clauses in their contracts[1985]. As part of the training, the controller could allocate data protection responsibilities to specific officers (e.g. chief infor-

---

1981 Actually, according to a Report requested by the European Commission, the most widely spoken mother tongues in 2012 were: German (16 %); Italian and English (13 % each), French (12 %), Spanish and Polish (8 % each). *See* this report by Special Eurobarometer 386 "Europeans and their languages" at <ec.europa.eu/ commfrontoffice/publicopinion/archives/ebs/ebs_386_en.pdf>. Last accessed 06/10/2021.

1982 The recommendation of the PRIPARE guidelines on accuracy and quality is to "ensure the quality of personal data collected, created, used, maintained and shared: when personal data is collected or created, confirm to the greatest extent practicable that it is accurate, useful, objective, relevant, timely and complete". *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, p. 124.

1983 *See* Chapter 3, Section 3.4.2.

1984 *See* e.g. the simplified model provided by the Italian DPA and the *modèle de registre simplifié* of the CNIL respectively at <www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9048342> and <www.cnil.fr/fr/ RGDP-le-registre-des-activites-de-traitement>. Last accessed 06/10/2021.

1985 An example of confidentiality agreement for French companies is provided by Commission Nationale de l'Informatique et des Libertés, *The CNIL's Guide on Security of personal data*, p. 6.

mation officer, data processing manager) by giving clear and documented instructions and by providing internal guidelines on data protection and security[1986]. It is highly advisable to define roles and responsibilities for managing data protection documentation and procedures[1987].

Before processing, the data controllers should prearrange the organisational chart to identify the subjects and categories of subjects and roles that can access the source systems and the EHR, and this register should be updated frequently. For example, in the hospital the persons involved in the patient's care, and then the users of the systems, change constantly. Entitlement creep should be avoided. Specific policies and procedures should be established for the creation, maintenance, and revocation of access[1988]. The data controller should also define a policy on authentication and passwords[1989]. The authorised roles should correspond to scalable levels of access, from mere access to administrative data to access to all the content of the EHR and source systems.

1986 Once again, the HIPAA rules are particularly valuable. *See* for a practical point of view chapter 25 of Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*.

1987 The PRIPARE guidelines on the accountability principle state that it is necessary to "establish an organization-wide privacy governance program: develop an organization-wide privacy plan which defines the strategies to implement privacy policies, controls and procedures. Develop operational privacy policies and procedures that govern the use of privacy controls. Disseminate privacy governance policies. Enforce the use of privacy controls as established by the privacy governance policies". *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, p. 129. The idea of the creation of privacy programmes is common in the US and in the FTC's actions. *See* e.g. Pardau and Edwards, "The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity".

1988 *See* Herold and Beaver, *The practical guide to HIPAA privacy and security compliance*, p. 335. *See* also Stevovic et al., "Enabling privacy by design in medical records sharing", p. 391, who propose this requirement for their project.

1989 As an example, the CNIL recommended adopting a user password policy that complies with its security recommendations provided in the *Délibération n. 2017–012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe*, and it requires a strong authentication mechanism with health professional cards or any alternative two-factor authentication tool. *See* Commission Nationale de l'Informatique et des Libertés, *Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux*, p. 9 and the *Délibération* at <www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>. Last accessed 06/10/2021. *See* also the security framework on authentication in Commission Nationale de l'Informatique et des Libertés, *The CNIL's Guide on Security of personal data*, pp. 7–9.

In addition, access rights and privileges should be adjusted in the access control policy according to data types (laboratory results, medications, prescription, medical history). Each role (e.g. nurse, surgeon) can have access to a limited set of data or to all data (e.g. general practitioner). It may be advisable that for booking and paying medical services sensitive data should be obscured from the administrative staff in light of data minimisation or they should be pseudonymised[1990]. So, the type of medical treatment or the related information of the scheduled test could be obscured or pseudonymised in the receipt. Anyway, health-related inferences might be made by the administrative staff. The duty of confidentiality upon employees and staff applies even beyond data protection issues in the contractual clauses on non-disclosure, and in the ethical professional codes[1991].

A complete security policy, a breach response plan and disaster recovery plan should be implemented and later reviewed periodically and at least once a year (Art. 32 GDPR)[1992]. The data controller should assign security responsibility to designated staff members (e.g. chief security officer). So, security and data breach management should not be limited to planning the policies applicable when a data breach occurs, but should be proac-

1990 *See* Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records", pp. 176–177.

1991 It may be specified that an ethics committee is frequently appointed in healthcare facilities to evaluate biomedical research and ethical issues. *See* e.g. the Operational Guidelines for Ethics Committees that review biomedical research of the World Health Organization, which were released in 2020 at <www.who.int/tdr/ publications/documents/ethics.pdf>. Last accessed 06/10/2021. The ethics committees should also evaluate the protection of research participant's confidentiality.

1992 According to Rezaeibagha, Win, and Susilo, "A systematic literature review on security and privacy of electronic health record systems: technical perspectives", p. 29, the application of security operations for the EHR system should include documented operating procedures, tests against malware, technical vulnerability management, testing of operational software, and checks and updates. Processes, procedures and tests should be established to ensure the availability of the system under adverse conditions. According to ENISA, in a high-risk processing the security policy should even be revised every six months. *See* European Union Agency for Network & Information Security, *Handbook on Security of Personal Data Processing*, p. 55; and European Union Agency for Network & Information Security, *ICT security certification opportunities in the healthcare sector*, p. 18, which includes an effective security policy, a disaster recovery plan and procedures for incident handling in the organisational measures for an HIT.

tive by defining procedures that can prevent a breach from occurring. Audits and check-lists should be used periodically to verify policies and procedures. Any breach should be documented thoroughly[1993].

Moreover, a certification mechanism may be a good voluntary means for ensuring trust in the systems (Artt. 25(3) and 42 GDPR)[1994]. The data controller could apply from a certification to the national accreditation body (Art. 43 GDPR)[1995]. Adopting a code of conduct may be another possible strategy (Artt. 24(3) and 40 GDPR).

During processing, in particular at the time of data collection, data controllers should find the applicable legal ground for the data processing (Art. 9 GDPR)[1996]. They should provide binding information to the data subject in the privacy policy[1997]. The privacy policy could be accessible in the EHR system and source systems. The privacy policy should be provided to data subjects either when their personal data are collected directly from them during a treatment or when they are obtained without their direct intervention. As an example, when a physician of the hospital accesses to the data collected in the EHR by the general practitioner, the privacy policy of the hospital under Article 14 of the GDPR should be provided to the patient. Other information may be provided later on request on the basis of the data subject's right to access.

According to data minimisation, purpose limitation, and accuracy principles, at the time of the collection and afterwards, the data controller should ensure that personal data are processed only as long as they are accurate, relevant, necessary and not excessive in relation to the purposes

---

1993 On security management *see* ISO/IEC 27001:2013, ISO/IEC 27035:2016, ISO 27799:2016, ISO 13606:2019, ISO/IEC 27007:2020.

1994 Some concrete examples of certifications are provided in European Union Agency for Network & Information Security, *Recommendations on European Data Protection Certification*, pp. 32–43.

1995 *See* Chapter 2, Section 2.5.3.

1996 In the PRIPARE project, a guideline of the purpose legitimacy and specification principle was "ensure legitimacy to collect and process personal data: collect, create, use, maintain, and share personal data, only if and to the extent authorized by a clearly defined legal basis (including user consent or any other legal basis). Collect, create, use, maintain, and share sensitive personal data only if and to the extent strictly authorized by a clearly defined legal basis that provides a relevant case for the collection of that sensitive personal data". *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, p. 122.

1997 This guideline also applies the "inform" strategy of Hoepman. *See* Hoepman, "Privacy Design Strategies (The Little Blue Book)".

for which they are collected and processed[1998]. This concept may be formalised in internal guidelines. At the same time, it should be noted that the EHR and its source systems should equally pursue the completeness of data concerning health to provide an efficient healthcare service to the patient on the "healthcare exception" ground.

Furthermore, during data processing activities data controllers should keep all documentation updated, including processing records. In particular, the privacy policy should be revised when practices or activities change. The data subject should have the opportunity to access or search the updated version of the privacy policy of the EHR and its source systems. Workforce training should be updated, too. It may be advisable that new training modules should be added once a year to take into account the new DPA's opinions or guidelines, soft law and rules established at the Member State and local level.

Performing a periodical gap analysis with the applicable legal requirements helps identify any changes that require new technical and organisational measures. Internal audits can periodically check compliance of the processing activities. If a data breach occurs, the response plan should be implemented to mitigate the effects and, where applicable, the breach should be communicated to the data subjects or to the DPA. All other subjects (e.g. processor, third parties) could be informed in order to assist the controller during the activities that mitigate the event. Moreover, when the data subject lodges a complaint or presents a request, the controller should respond to the subject in a reasonable timeframe and by commonly used means[1999].

Finally, after processing, meaning if the data controllers stops using the EHR and personal data are deleted or anonymised, Article 25 does not apply. However, it should be noted that this condition happens only if data are appropriately de-identified by removing all the identifiers and all

1998 In the PRIPARE project, the guideline of collection limitation was: "limit the personal data collected to the strict minimum consented and necessary. When personal data is collected or retained, require only those personal data that are relevant and necessary for the purpose that has been previously identified, authorized and consented by the data subject. Suitably specify the purpose for which the personal data can be used and the rationale for that. When personal data is processed, only process it for the purpose for which it was originally obtained, or for purposes compatible with it". *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, p. 122.

1999 Recital 59 GDPR states that the request should be answered in one month.

details[2000]. So, appropriate technical solutions should be implemented to avoid any abuse to ineffective anonymisation of data concerning health. Moreover, this category of data is frequently associated with an unlimited or very long data retention period. Actually, the data subject may not have the right to erasure of data concerning health in the EHR context[2001]. Therefore, the measures should be implemented even beyond the lifetime of the data subject and beyond the period of the healthcare treatment or service.

This section has explained how to apply Article 25 in the EHR context and presented several guidelines. The following section classifies the set of guidelines to be implemented before and during data processing activities and assigns data protection principles.

6.4 The set of guidelines

Technical requirements and goals are defined in the following Tables 6.1 – 6.6. The organisational requirements follow in Tables 6.7 – 6.11. Descriptions and data protection principles (and rights) juxtapose the set of guidelines[2002].

2000 *See* e.g. the list of identifiers of the HIPAA in Chapter 4, Section 4.4.1.

2001 The data should be retained under Member State law at least in paper form. *See* Chapter 3, Section 3.4.2.

2002 The manner in which the classification of the measures is provided can be compared with the typical ENISA annex where the authority presents proposed measures in a large table with "measure category, measure identifier, measure description, relevant standards" as columns. *See* European Union Agency for Network & Information Security, *Handbook on Security of Personal Data Processing*.

Table 6.1 DPbD technical guidelines of data at rest before processing

MEASURE	DESCRIPTION	PRINCIPLE
Map data flows in the projected EHR	Data controllers should have clear data flows in the EHR environment and source systems	Accountability and security, data minimisation
Separate administrative personal data from sensitive data at the database level	Data controllers should implement this separation of databases during EHR development	Confidentiality and integrity, data minimisation
Separate sensitive data from particularly sensitive data at the database level	Data controllers should implement this separation of databases during EHR development	Confidentiality and integrity
Encrypt the EHR database	Data controllers could encrypt the EHR system (full disk) or their databases at the file system level	Confidentiality and integrity
Implement back-up and recovery mechanism	Data controllers should implement back-up and recovery mechanisms	Integrity
Implement intrusion control system	Data controllers should implement an efficient intrusion control system	Confidentiality and integrity
Implement audit and log systems	Data controller should implement efficient audit and log system for collecting ID number, date and hour, type of operation and reason for access of an event in the EHR	Accountability, integrity and confidentiality, transparency

Table 6.2 DPbD technical guidelines of data at rest during processing

MEASURE	DESCRIPTION	PRINCIPLE
Review the solutions adopted before processing	Data controllers should technically review the implemented solutions frequently	Integrity, confidentiality, accountability
Back up personal data on a daily basis and the entire system on a monthly basis	Data controllers should back up personal data at least daily and the systems monthly	Integrity and availability
Carry out periodic penetration tests	Data controller should carry out penetration tests periodically	Integrity

Table 6.3 DPbD technical guidelines of data in use before processing

MEASURE	DESCRIPTION	PRINCIPLE
Implement an access control system	Data controllers should choose an efficient and appropriate access control mechanism for the authorisation of the users in the systems	Integrity and confidentiality
Define identity management system	Data controllers should choose an efficient and appropriate mechanism to identify users in the systems	Integrity and confidentiality
Use appropriate authentication mechanism	Data controllers should choose an efficient and appropriate mechanism for the authentication of users in the systems	Confidentiality and data minimisation

MEASURE	DESCRIPTION	PRINCIPLE
Implement multiple modules of presentation of data in the interface	Data controllers should differentiate between different types of data at the interface level	Confidentiality

Table 6.4 DPbD technical guidelines of data in use during processing

MEASURE	DESCRIPTION	PRINCIPLE
Pseudonymise data concerning health	Data controller should pseudonymise data concerning health to minimise use by unauthorised users	Data minimisation
Create a prompt on the legal ground in the interface	The EHR system and the source systems should prompt the user to obtain patient consent or define a legal ground	Lawfulness
Use a consent mechanism	Where applicable, data controllers should use a consent mechanism to obtain consent in a machine-readable form	Lawfulness
Use the anomaly detection tool and the automated monitoring system	Data controller should monitor the log files	Confidentiality and integrity
Use the automatic alert system on legal ground	When the legal basis ceases to apply, the event should be flagged in the system and stopped until a new legal ground applies	Lawfulness

MEASURE	DESCRIPTION	PRINCIPLE
Create an electronic access mechanism for the data subject or secure message service	Data controllers should implement a secure mechanism for granting access and a copy of data to the data subjects	Accountability, right to access
Create a mechanism to conceal specific data	Where applicable, data controllers should conceal specific data concerning health whose access is limited	Accountability, right of concealment
Ensure data portability	Where applicable, data controllers should transmit data to other controllers	Accountability, right to data portability

Table 6.5 DPbD technical guidelines of data in transit before processing

MEASURE	DESCRIPTION	PRINCIPLE
Implement a secure transmission network	Data controllers should implement mechanisms to secure the EHR network	Confidentiality and integrity
Implement the existing tools provided by the eHDSI	Data controllers should implement the EC's exchange format tools to ensure interoperability across Member States of patient summary, laboratory results, medical imaging and reports, and hospital discharge reports	Accountability

Table 6.6 DPbD technical guidelines of data in transit during processing

MEASURE	DESCRIPTION	PRINCIPLE
Monitor the secure transmission network	Data controllers should monitor the mechanisms to secure the EHR network	Confidentiality and integrity

Table 6.7 DPbD organisational guidelines before processing 1

MEASURE	DESCRIPTION	PRINCIPLE
Determine the status	The subjects should determine whether they fall under the scope of the GDPR, and under which status (controller or processor)	Applicability
Perform a gap analysis on the rules	Data controllers should analyse the applicable legal requirements	Applicability
Evaluate the state of the art	Data controllers should understand what corresponds to the state of the art of technologies and organisational practices	Taking into account the state of the art
Identify the nature, scope, context and purposes of the processing	Data controllers should analyse the concrete characteristics of their data processing activities	Taking into account the nature, scope, context and purposes
Identify the risks posed by the processing	Data controllers should identify the risks for rights and freedoms of individuals beyond the DPIA	Taking into account the risks of varying likelihood and severity, fairness

MEASURE	DESCRIPTION	PRINCIPLE
Establish a DPbD compliance budget	Data controllers should estimate the costs and allocate resources to implement the measures	Taking into account the cost of implementation
Use a certification mechanism	Data controllers could apply for a certification from national accreditation bodies	Accountability and transparency
Authorise the processor's activities	The controllers should authorise the processor on the delegated activities in written form	Accountability
Stipulate the contract with the processor	Data controllers should stipulate contracts or other legal acts with the processors	Accountability
Where applicable, stipulate the agreement with joint data controllers	Joint controllers should stipulate an agreement to determine the respective responsibilities	Accountability

Table 6.8 DPbD organisational guidelines before processing 2

MEASURE	DESCRIPTION	PRINCIPLE
Perform the DPIA	Data controllers should perform a DPIA, except in the case of individual healthcare professionals	Accountability
Identify the DPO	Data controllers should designate a DPO, which may be a unique subject for the EHR environment	Accountability
Assign data protection tasks and allocate responsibilities to specific staff and third parties	Data controllers should assign duties on data protection management to specific internal staff or third parties	Accountability
Create a record of the processing activities	Data controllers should create a record of processing activities	Accountability
Conduct appropriate levels of training for staff	Data controllers should train their workforce and staff members on data protection and security	Accountability
Define the categories of particularly sensitive data	Where still not provided by law, data controllers could identify particularly sensitive data	Confidentiality and accountability

MEASURE	DESCRIPTION	PRINCIPLE
Create an access control policy	Data controllers should establish the identity, roles and categories of users having access to the source systems and to the EHR and adjust access rights and privileges	Confidentiality, data minimisation
Create a specific policy on monitoring access	Data controllers should define policies and procedures related to maintaining and revoking access rights and privileges	Confidentiality
Create a specific policy on authentication	The data controller should also define a policy on authentication and passwords	Confidentiality

Table 6.9 DPbD organisational guidelines before processing 3

MEASURE	DESCRIPTION	PRINCIPLE
Document compliance activities	Data controllers should document the compliance activity at the organisational level	Accountability
Create the privacy policy	Data controllers should create the privacy policies	Transparency
Define the policy on data accuracy	Data controllers should define procedures and policies applicable to ensuring the accuracy of personal data	Accuracy

MEASURE	DESCRIPTION	PRINCIPLE
Define the applicable data retention policy	Data controllers should define procedures and policy applicable to defining the data retention period	Storage limitation
Create the policy for the exercise of data subject's rights	Data controllers should define procedures and policy applicable to handling data subject's requests	Accountability
Create the policy on the communication of data protection events	Data controllers should define procedures and policies for communicating a data breach to the data subjects	Accountability and transparency
Create the policy on notification of data protection events	Data controllers should define procedures and policies for communicating a data breach to the DPA	Accountability
Create the policy for replying to the DPA or public requests	Data controllers should define procedures and policies applicable for requests from the DPA or other authorities	Accountability
Create the policy on security, the data breach response plan and the disaster recovery plan	Data controllers should define procedures and policies on security	Integrity, confidentiality, and availability
Create the policy on disclosures	Data controllers should define procedures and policy applicable to disclosures required by law	Accountability and confidentiality, data minimisation

Table 6.10 DPbD organisational guidelines data collection

MEASURE	DESCRIPTION	PRINCIPLE
Identify the legal ground	Data controllers should define a legal ground for every processing activity and related purpose	Lawfulness
Where applicable, obtain explicit consent	If Member State law requires consent, the data controller should obtain explicit consent, which is separate from consent to the treatment or to secondary uses of the EHR	Lawfulness
Inform data subject	Data controllers should provide the privacy policies to data subjects	Transparency
Apply limits to the collection	Data controllers should collect only accurate data that are necessary for limited and defined purposes. Internal guidelines should be established in this regard	Purpose limitation, data minimisation, accuracy

Table 6.11 DPbD organisational guidelines during processing

MEASURE	DESCRIPTION	PRINCIPLE
Document compliance activities	Data controllers should document compliance activity at the organisational level	Accountability
Maintain a record of processing activities	Data controllers should maintain a record of processing activities	Accountability
Update the levels of training for staff	Data controllers should train their workforce on the data protection framework	Accountability
Audit the processors and third parties	Data controllers should audit the compliance of processors and third parties	Accountability
Update privacy policies and any other data protection documents	All documents should be revised periodically	Transparency
Update inaccurate data and delete data after the retention period	Data controllers should keep data up-to-date and delete them when the retention period is finished	Accuracy, storage limitation
Perform periodic gap analysis with the rules	Data controllers should monitor the applicable legal requirements	Applicability
Perform regular internal audits for each aspect of compliance	Data controllers should monitor compliance at the organisational level, including periodically reviewing policies and procedures on security	Accountability

MEASURE	DESCRIPTION	PRINCIPLE
Perform periodic risk assessment that addresses new risks	Data controllers should assess new risks	Taking into account the risk
Where applicable, communicate and notify a data breach	Data controllers should communicate and notify a data breach in the presence of high risks	Accountability
Respond to requests and complaints from individuals	Data controllers should define procedures and policies applicable to handling the data subject's requests and complaints	Accountability

6.5 Notes on liability issues: possible scenarios

The obligation to implement DPbD measures is on data controllers. However, other subjects are involved in the concrete implementation: the processor, the developer, the DPO, third parties, internal officers and the workforce in general (medical or administrative staff). This section provides some brief notes on liability in the event of inappropriate or ineffective DPbD implementation.

The GDPR establishes administrative fines for violations of the legal requirements that cause material or immaterial harm to data subjects, including the DPbD obligation[2003]. Article 82(1) – (2) GDPR introduces the right to compensation and liability as follows:

2003 *See* Chapter 2, Section 2.4. On the GDPR framework on sanctions *see* Gabriela Zanfir-Fortuna. "Chapter VIII Remedies, Liability and Penalties (Articles 77–84). Article 82. Right to compensation and liability". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 1160–1179. ISBN: 9780198826491; Waltraut Kotschy. "Chapter VIII Remedies, Liability and Penalties (Articles 77–84). Article 83. General conditions for imposing administrative fines". In: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, pp. 1180–1193. ISBN: 9780198826491; Orla Lynskey. "Chapter VIII Remedies, Liability and Penalties (Articles 77–84). Article 84. Penalties". In: *The EU General Data Protection Regu-*

"1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller".

As regards DPbD, the data controller is liable under Article 83(2)(d) and (4)(a) of the GDPR, when it causes a damage by its processing[2004]. Pur-

---

lation (GDPR): A Commentary. Oxford University Press, 2020, pp. 1194–1201. ISBN: 9780198826491; Emilio Tosi. "Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo". In: *Contratto e Impresa* 3 (2020), pp. 1115- 1151; Emilio Tosi. *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*. Giuffrè Francis Lefebvre, 2019. ISBN: 9788828817192; Emilio Tosi. "La responsabilità civile per trattamento illecito dei dati personali". In: *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*. Giuffrè Francis Lefebvre, 2019, pp. 619–675. ISBN: 9788828811381; Giovanni Mulazzani. "Le sanzioni amministrative in materia di protezione dei dati personali nell'ordinamento europeo ed in quello nazionale". In: *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*. Zanichelli, Torino, 2019, pp. 768–795. ISBN: 9788808820433; Panetta, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)*, pp. 435–444; Fabio Bravo. "Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali". In: *Persona e mercato dei dati. Riflessioni sul GDPR*. Wolters Kluwer, 2019, pp. 384–418. ISBN: 9788813370510; Voigt and Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, pp. 201–217. On sanctions in the healthcare field *see* Giovanni Comandé and Denise Amram. "La violazione della privacy in sanità, tra diritto civile e diritto penale". In: *Itinerari di medicina legale e delle responsabilità in campo sanitario*. G. Giappichelli Editore, 2021. ISBN: 9788892132634.

2004 Article 83(2) establishes that "administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following (...)", including (d) which introduces Article 25: "the degree of responsibility of the controller or processor taking into account technical and

suant to Article 82(3) GDPR, the controller can be exempted from liability if it proves that it is not in any way responsible for the event giving rise to the damage[2005]. According to Tosi, GDPR liability is a particular form of strict liability since the rules consider processing inherently dangerous and create a reversal of the burden of proof[2006]. At the same time, it might be argued that if the measures had been adequate, the damage would not have occurred[2007].

First of all, it may be highlighted that the broad discretion for data controllers on DPbD implementation leaves enough space for courts to rule and on DPAs to sanction. On the one hand, the adequacy of the measures is related to an objective case-by-case evaluation of the court or the DPA. On the other hand, DPbD implementation is performed on a case-by-case

---

organisational measures implemented by them pursuant to Articles 25 and 32".

2005 *See* also Recital 146 GDPR: "The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing".

2006 *See* Tosi, "Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo", p. 1131; Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*; Tosi, "La responsabilità civile per trattamento illecito dei dati personali", pp. 657–659. The author argues that proof is a so-called *probatio diabolica*, i.e. a proof that is very hard to prove.

2007 Tosi, *op. cit.*, p. 658, where the author highlights that this is a statement coming from reasoning that pre-empts a legal interpretation.

basis, and the criteria to be taken into account are mainly subjective. Thus, finding arguments for contesting compliance with Article 25 seems neither easy nor immediate[2008].

The state of the art of PETs and measures changes over time. The cost of implementation is a complex criterion to evaluate. The risk assessment and the concrete characteristics of processing are highly subjective. Therefore, compliance checking has been defined as a "moving target"[2009]. All the criteria of Article 25 will be taken into account during the judgement to ascertain the interruption of the causal link between the data controller's processing operations and adopted measures and the occurred damage[2010]. The controller will be liable when the data processing is not compliant with the obligation and the damage is caused by this processing[2011].

In 2019 and 2020 some DPAs started to sanction data controllers for non-compliance with the requirements of Article 25. A few interesting investigations and proceedings can be reported and briefly analysed here.

In 2019, the Romanian DPA sanctioned Unicredit Bank S.p.A. on the basis of Article 25(1) GDPR for failing to implement appropriate technical and organisational measures. In particular, the data controller disclosed data concerning personal identification numbers and payers' addresses during external and internal transactions of 337,042 data subjects without appropriate and adequate measures to control the data processing opera-

2008 Bygrave claimed that heavy sanctions related to Article 25 are difficult to handle since the language of the provision is vague and relatively abstract. *See* Bygrave, "Chapter IV Controller and Processor (Articles 24–43). Article 25. Data protection by design and by default", p. 579. At that time, the author quoted the decision of the Romanian DPA of 27 June 2019 to support the belief that controllers cannot escape compliance with DPbD. On this deliberation *see* the next paragraphs.

2009 *See* Schiffner et al., "Towards a roadmap for privacy technologies and the General Data Protection Regulation: A transatlantic initiative", p. 28.

2010 *See* Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, pp. 75–76.

2011 As an example, according to Bravo who uses Italian civil law categories, this obligation is an "*ex lege* obligation", since it is generated from a fact or an act acknowledged by law as generating the legal obligation established by a provision. In particular, it is an "obligation to act" that protects personal data ("obblighi protettivi"). This category is derived from the German doctrine and is also used in the Italian legal system. *See* Bravo, "Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali", pp. 404–414.

tions[2012]. The data controller failed to appropriately implement the data minimisation principle with effective measures at the time of the data processing activities.

In the same year, the Berlin Commissioner for Data Protection investigated the data processing carried out by the real estate company Deutsche Wohnen SE. The configuration of the archive systems used by this data controller did not ensure that personal data were kept for no longer than was necessary for the specified purposes[2013]. The Commissioner sanctioned the company for over 14 million Euro on the basis of Article 25 GDPR. The data retention system was ruled to be as inappropriate as such, even before the occurrence of a data breach. In this particular case, the controller failed to implement the storage limitation principle with appropriate measures.

High fines have been imposed in the telecommunication sector[2014]. In 2019 the Hellenic DPA sanctioned the Hellenic Telecommunications Organization on the basis of Articles 5(1)(c) and 25(1) GDPR for failing to implement appropriate organisational measures to control processing activities related to advertisement purposes and to the recipients of consumer contact lists[2015]. Personal data of former consumers were included in the registers for telemarketing purposes, used for unsolicited promotional calls, and not deleted after requests. In 2020, the Italian DPA found Vodafone Italia S.p.A. to have violated Article 5(1) – (2) and Article 25(1) GDPR due to its failure to implement appropriate technical and organisational measures to test and ensure compliance of the collection of personal data from the first phase of data processing, despite the signifi-

---

2012 On the decision of this DPA *see* the official website at <www.dataprotection .ro/index.jsp?page=Comunicat_ Amenda_Unicredit&lang=en>, and the press release of the EDPB at <edpb.europa.eu/news/national-news/ 2019/first-fine-romanian-supervisory-authority_en>. Last accessed 06/10/2021.

2013 *See* the official press release at <www.datenschutz-berlin.de/filead min/user_upload/pdf/pressemitteilungen/2019/20191105-PM-B ussgeld_DW.pdf>; and the press release of the EDPB at <edpb.europa.eu/news/ national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_it>. Last accessed 06/10/2021.

2014 *See* the statistics by CMS and available at <www. enforcementtracker.com/?insights>. Last accessed 06/10/2021.

2015 *See* decision no. 31/2019 at <www.dpa.gr/el/enimerwtiko/prakseisArxis/ epiboli-prostimoy-se-etaireia-parohis-ypiresion-tilefonias-gia-parabiasi>; and the press release of the EDPB at <edpb.europa.eu/news/national-news/2019/ administrative-fines-imposed-telephone-service-provider_en>. Last accessed 06/10/2021.

cant number of complaints and alerts[2016]. Actually, the company violated many requirements of the GDPR[2017]. As regards the DPbD obligation, the Italian DPA held that the telemarketing activities and the first contacts with several potential customers (data subjects) that were carried out by operators of the sales network and by tele-marketers were not continuously performed in compliance with the GDPR[2018]. In particular, the control systems did not exclude the existence of subscriptions to contracts and service activation from unlawful and unsolicited telemarketing calls[2019]. The processing operations resulted in aggressive telemarketing practices towards data subjects. Interestingly, the authority explained that key elements of the data protection by design obligation include attention to prevention, functionality, security, transparency and centrality of the data subjects' interests. The Italian DPA held that the data controller did not adopt appropriate measures to exclude and mitigate risks by explaining how systems should have been designed to effectively monitor the data processing operations. On top of a 12 million Euro administrative fine, Vodafone received the order to adjust measures and access systems to secure its databases. In the same year and industry, the Italian DPA sanctioned other telecommunications companies (TIM S.p.A.[2020], Iliad Italia S.p.A.[2021] and Wind Tre S.p.A.[2022]) on the basis of several articles of the GDPR, including Article 25, for failing to integrate appropriate technical and organisational measures in their data processing activities.

2016 Garante per la protezione dei dati personali, Provvedimento del 12 novembre 2020, published in Registro dei provvedimenti n. 224 del 12 novembre 2020, available at <www.ItalianDPAprivacy.it/web/guest/home/ docweb/-/docweb-display/docweb/9485681>. Last accessed 06/10/2021.

2017 *See* for more details Bincoletto, "Italy – Italian DPA Against Vodafone: History of a €12 million Fine".

2018 *See* Bincoletto, *op. cit.*, p. 556.

2019 *See ibid.*

2020 Garante per la protezione dei dati personali, Provvedimento del 15 gennaio 2020, published in Registro dei provvedimenti n. 7 del 15 gennaio 2020, available at <www.garanteprivacy.it/web/guest/home/docweb/-/ docweb-display/docweb/9256486>. Last accessed 06/10/2021.

2021 Garante per la protezione dei dati personali, Provvedimento del 9 luglio 2020, published in Registro dei provvedimenti n. 138 del 9 luglio 2020, available at <www.garanteprivacy.it/home/docweb/-/docweb-display/ docweb/9435807>. Last accessed 06/10/2021.

2022 Garante per la protezione dei dati personali, Provvedimento del 9 luglio 2020, published in Registro dei provvedimenti n. 143 del 9 luglio 2020, available at <www.garanteprivacy.it/home/docweb/-/docweb-display/ docweb/9435753>. Last accessed 06/10/2021.

In the e-health care sector, in 2020 the Swedish DPA sanctioned seven healthcare providers for failing to conduct assessments and risk analysis on processing with electronic health records systems, limit the access level of users, and implement appropriate security measures[2023]. The DPA did not apply Article 25, but Articles 5, 24 and 31 GDPR. However, it is interesting to report these decisions since, on the one hand, they show that the DPIA, the access control system, and the identity management system are pivotal in the context of EHRs; on the other hand, the measures for limiting authorisation to access the EHR should be implemented from the design stage of the systems and should actually result from the application of DPbD. In fact, on December 2020 the Norwegian DPA sanctioned the Østfold HF Hospital on the basis of Articles 25 and 32 for unappropriated access control and management system of patients' lists in the years 2013–2019[2024].

As pointed out by Hielke Hijmans, President of the Litigation Chamber of the Belgian DPA, the GDPR does not apply only to companies, but also to citizens[2025]. The implementation of Article 25 concerns all data processing under the GDPR. The Belgian DPA sanctioned a couple of private individuals who had installed a video surveillance system on their property consisting of five cameras on the basis of improper placement of two of these cameras[2026]. The proceeding started with the complaint by two neighbours who noticed that surveillance cameras were filming part of the public highway and their private property and that the couple had

---

2023 *See* <www.imy.se/nyheter/brister-i-hur-vardgivare-styr-personalens-atkomst-till-journaluppgifter/>; and the press release of the EDPB at <edpb.europa.eu/news/national-news/2020/ deficiencies-how-healthcare-providers-control-staff-access-patient-journal_en>. Last accessed 06/10/2021.

2024 *See* the decision at <www.datatilsynet.no/contentassets/580ab399d02d4d369de8c5905757d4b2/~-20_02291-4-vedtak-om-overtredelsesgebyr-og-palegg-208484_13_1.pdf>; and the press release of the EDPB at <https://edpb.europa.eu/news/national-news/2020/ norwegian-dpa-imposes-administrative-fine-ostfold-hf-hospital_en>. Last accessed 06/10/2021.

2025 *See* the press release of 25 November 2020 at <https://www.autoriteprotectiondonnees.be/citoyen/ lapd-impose-une-amende-pour-traitement-illegitime-dimages-de-cameras-de-surveillance>. Last accessed 06/10/2021.

2026 *See* the official press release at <https://www.autoriteprotectiondonnees.be/citoyen/ lapd-impose-une-amende-pour-traitement-illegitime-dimages-de-cameras-de-surveillance>. The decision is available in Dutch at <https://www.autoriteprotectiondonnees.be/publications/ decision-quant-au-fond-n-74–2020.pdf>. *See* also the press release of the EDPB at <https://edpb.europa.eu/news/national-news/2020/belgian-dpa-fine-unlawful-processing-video-images_en>. Last accessed 06/10/2021.

use some captured pictures during an administrative dispute procedure regarding environmental planning by transferring data to an external expert. The Belgian DPA found that images (i.e. personal data) were collected and disclosed by transmission without a lawful legal ground for processing. The legitimate interest of the couple in protecting their property and domestic context did not justify filming the public highway or the property of others and using the images in a dispute procedure. The couple, as data controller, should have properly placed the cameras. According to this authority, the controller infringed Article 25(1) GDPR due to this improper placement.

The brief analysis of the above mentioned investigations and proceedings shows once again that compliance with Article 25 is strictly related to the appropriate implementation of data protection principles. Authorities may contest compliance in every aspect of data processing and evaluate the adopted measures item by item. In the future, DPAs might release specific guidelines or opinions on DPbD obligations at the enforcement level to explain their approaches to evaluating the measures of Article 25.

Secondly, some considerations should be provided for each category of subjects.

When in the EHR environment there are joint controllers, their agreement should specify the respective duties and responsibilities (Art. 26 GDPR). It is important to allocate responsibilities for the implementation of DPbD technical and organisational measures. The data subjects have the possibility to exercise their rights against each controller. In fact, each controller remains responsible for any damage caused by the processing, and each subject is liable for the entire damage[2027]. This is a case of joint and several liability[2028].

As regards the processor, this subject is typically a contractor or the outsourcing company that manages the ICT systems (e.g. external service provider). The data controller should carefully choose a processor that is able to provide guarantees of compliance[2029]. In fact, the controller may

2027 *See* Article 82(4) GDPR.

2028 *See* Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, p. 43. Internally, it will be necessary to investigate the different causal contribution of each controller. Then, the compensation for damages will be divided between the joint controllers according to the different levels of liability. *See* also Tosi, "La responsabilità civile per trattamento illecito dei dati personali", p. 650.

2029 *See* Dimitri De Rada. "La responsabilità civile in caso di mancato rispetto del GDPR. Privacy by default, privacy by design e accountability nell'ottica del

be liable for *culpa in eligendo et in vigilando* when the subject chooses a processor that does not provide the appropriate guarantees[2030]. The processor's duties are defined in the contract or legal act adopted pursuant to Article 28 GDPR between this subject and the data controller.

According to Article 82(2) GDPR, the processor can be liable for any damage caused by processing when specific obligations that the GDPR places on its role are not fulfilled, e.g. the implementation of security measures[2031]. When the processor engages a sub-processor, this subject remains fully liable to the data controller for the performance of the processor's duties pursuant to Article 28(4) GDPR[2032]. Moreover, the processor is liable when this subject acts in a manner that is inconsistent with or contrary to the instructions given by the data controller in their contract. This last scenario may actually establish a joint liability between the controller and the processor. Where all these scenarios do not apply, and the data controller has been fined for violation of Article 25 GDPR, this subject may still sue the processor in a recourse action on the basis of the contract and under civil or private law. The processor should demonstrate that they followed the instructions and adopted the appropriate measures.

Beyond the elements listed in Article 28(3)(c) and (e) GDPR, it may be argued that the contract between the processor and the controller should specifically stipulate that the processor should assist the controller for the fulfilment of the obligations of Article 25 GDPR by appropriate

---

Diritto Privato". In: *Federalismi.it* 23 (2019), pp. 1–16, p. 10, which considers this contract a DPbD measure in itself. In the Guidelines on Article 25 the EDPB recommends on the one hand that controllers "should not choose producers or processors who do not offer systems enabling or supporting the controller to comply with Article 25, because controllers will be held accountable for the lack of implementation thereof"; on the other hand, the authority recommends "controllers to require that producers and processors demonstrate how their hardware, software, services or systems enable the controller to comply with the requirements to accountability in accordance with DPbDD, for example by using key performance indicators to demonstrate the effectiveness of the measures and safeguards at implementing the principles and rights". *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 30. So, the controller should seek guarantees and be very careful in their choice.

2030 *See* Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, pp. 60–61.

2031 *See* once again Article 28 GDPR.

2032 According to Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, p. 63, the designation is *tamquam non esset* for the controller from a liability point of view.

and effective technical and organisational measures. The controller that processes data concerning health may choose a processor that has received a certification or uses a code of conduct[2033].

The developer is a role that the GDPR takes into account only in Recital 78 to encourage an application of DPbD and DPbDf beyond the duty of the data controllers[2034]. A contract usually regulates the relation between the developer and the customer, which may be either the processor or the data controller. This contract is regulated under Member State law, private law and commercial law especially.

In that contract, the parties may include a specific declaration on the application of the GDPR requirements and of the principle of DPbD[2035]. In particular, the controller may ask the developer to write a statement to prove that its product (e.g. the source system and/or the EHR system) has been analysed on the basis of GDPR requirements and that the adequacy analysis demonstrates that it complies with these regulatory requirements. The contract could otherwise make reference to specific standards to be adopted during development. As a result, the standards or the DPbD implementation will be part of the contractual agreement and will bind the developer from a private or civil law perspective. A controller who has been fined under the GDPR could enforce the DPbD requirement on contractors and service providers when this requirement was documented in the contract[2036]. However, under the GDPR and against the data subjects, the data controller remains the only subject liable for the violation.

Another subject that inevitably and actively participates in the DPbD implementation is the DPO, who advises the controller and processor on the obligations to carry out, including DPbD[2037]. Since the DPO shall

2033 Article 28(5) GDPR establishes that a certification or a code of conduct could be used for demonstrating the provision of guarantees by the processor. The use of codes of conducts, standards and certification is highly recommended by the EDPB in European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 30.

2034 *See* Chapter 2, Section 2.4.1.

2035 The CNIL recommended including specific clauses in sub-contractors' contracts in Commission Nationale de l'Informatique et des Libertés, *Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux*, p. 10.

2036 In the PRIPARE's guidelines on accountability, it is recommended to "include privacy requirements in documents related to contracts, procurement and acquisition". *See* Notario et al., *PRIPARE. Privacy-and Security-by design Methodology Handbook. 2016*, p. 130.

2037 *See* Article 39 GDPR.

monitor compliance with the GDPR requirements and with the internal policies and procedures, the officer shall control the implementation of the DPbD measures. The DPO shall especially monitor the DPbD implementation at the organisational level, including the risk assessment level. The EDPB encourages the active involvement of the office on DPbD and DPbDf activities in the whole processing life-cycle[2038]. When the DPO does not perform these tasks, this officer may be liable to the data controller and the processor under contract law for lack of professional diligence[2039].

Finally, during processing third parties and internal workforce may process personal data on behalf of the controller and they may not implement the required measures. Since the controller will remain liable under the GDPR, it is necessary to stipulate specific confidentiality clauses in the contracts and other clauses that establish the duty to follow internal procedures and guidelines to guarantee the fulfilment of technical and organisational DPbD measures.

Despite the complexity of Article 25 and of the enforcement level, the data controller should carefully apply this requirement and be protected at a contractual level since the administrative fines set by the GDPR could have a great impact on their business, especially if they are SMEs[2040].

2038 *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 29.

2039 *See* Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, pp. 89–91.

2040 The EDPB suggests the following steps for SMEs: "do early risk assessments; start with small processing – then scale its scope and sophistication later; look for producer and processor guarantee of DPbDD, such as certification and adherence to code of conducts; use partners with a good track record; talk with DPAs; read guidance from DPAs and the EDPB; adhere to codes of conduct where available; get professional help and advice". *See* European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 30.