Medicine, Science and the Law

The European General Data-Protection Regulation (GDPR) in mHealth. Theoretical and practical aspects for Practitioners' use.

Journal:	*Medicine, Science and the Law*
Manuscript ID	MSL-22-043
Manuscript Type:	Review Article
Date Submitted by the Author:	02-Mar-2022
Complete List of Authors:	Carmi, Lior; Reichman University, Data science Zohar, Mishael; Reichman University Riva, Gianluigi; University College Dublin
Keywords:	GDPR;, Mobile health;, Digital monitoring;, Digital health, Privacy

Abstract:	The extensive use of smart technology (smartphones & wearables) and the vast amount of information they contain, has positioned remote devices and technology as a massive database resource. Harnessing this big data into the clinical and research fields has introduced a new horizon of possibilities along with significant privacy issues. A significant evolution in this respect has been the introduction of the new European Union (EU) General Data Protection Regulation (GDPR). The GDPR acknowledges that information related to individuals (i.e., personal data), as well as data flow, and thus databases, are of high political, clinical, and economic value. Hence, the Regulation aims to protect personal data and, consequentially, privacy. Nevertheless, the GDPR is a legal document with legal language. The purpose of this paper is to serve as a - practical guidance as well as a theoretical framework -for clinicians (and non-clinicians) who integrates digital tools in their clinical and research work.

The European General Data-Protection Regulation (GDPR) in mHealth. Theoretical and practical aspects for Practitioners' use.

Carmi, Lior[1]., Zohar, Mishael[1] and Riva Gianluigi M.[2].

[1.] The Data Science Institution, Reichman University, Herzliya, Israel

[2.] University College Dublin, School of Information and Communication Studies, Dublin, Ireland.

Corresponding Author: Dr. Lior Carmi, Reichman University, HaUniversita 8 8, Herzliya, 4610101, Israel. Phone: +97235186207 Fax: +97235186091 Mobile: +972502211969. Email: Lior.carmi@outlook.com .

Number of words: 4358

The implications of the European GDPR in mobile Health

Abstract

The extensive use of smart technology (smartphones & wearables) and vast amount of information they contain, has positioned remote devices and technology as a massive database resource. Harnessing this big data into the clinical and research fields has introduced new horizon of possibilities along with significant privacy issues. A significant evolution in this respect has been the introduction of the new European Union (EU) General Data Protection Regulation (GDPR). The GDPR acknowledges that information related to individuals (i.e., personal data), as well as data flow, and thus databases, are of high political, clinical, and economic value. Hence, the Regulation aims to protect personal data and, consequentially, the privacy. Nevertheless, the GDPR is a legal document with legal language. The purpose of this paper is to serve as a - practical guidance as well as theoretical framework -for clinicians (and non-clinicians) who integrates digital tools in their clinical and research work.

Keywords: GDPR; Mobile health; Digital monitoring; Digital health, Privacy.

The implications of the European GDPR in mobile Health

Introduction to the Legal Privacy understanding

The widespread use of digital tools opens new clinical possibilities but also raises new hazards, including increased concern regarding privacy. On May 25th, 2018, a significant evolution has been introduced to the individuals' privacy protection with the coming into effect of the new European Union (EU) General Data Protection Regulation (GDPR) [1]. The GDPR acknowledges that information related to individuals (i.e. personal data), as well as data flow, and thus databases, are of high political, clinical, and economic value. This consequently raises concern about possible abuses of information exploitation and other misconducts related to personal data processing [2]. Hence, the Regulation aims to protect personal data and, consequentially, the privacy of EU citizens.

Commented [A1]: Not only EU citizens, but individuals who are resident in EU

In Europe, the term "Privacy" (When capitalized refers to the whole legal regime for the matter) usually refers as a general legal domain, although it contains the unsolved overlap between Privacy and Data Protection (DP). In Civil Law systems (upon which the EU regulatory system is designed), Privacy refers back to personhood rights, such as dignity, name, image and so on, while Data Protection, on the other hand, is connected to the governance of data processing. Both are fundamental rights provided by the EU Charter of Fundamental Rights (Articles 7 and 8), and this involves that the EU system accords the maximum level of protection for the Privacy realm. This means that Privacy entails personhood rights, whereas Data Protection provides protection to them.

A further complication for non-legal practitioner for correctly understanding privacy, is represented by the different privacy conceptualization between the United States and the European Union. According to the US approach, an individual owns his data (and, so, his privacy) according to a proprietary paradigm, and therefore, once data are contractually yielded the individual cannot claim other rights on them (i.e. a proprietary paradigm) as the appear to

be sold [3, 4]. Accordingly, in the US applies the so-called "third-party doctrine", which states that if one publicly released their personal data, they lose their rights on them and third parties can exploit the data freely. Furthermore, the US holds a libertarian economic model, therefore, the exploitation of personal data for commercial purposes is highly tolerated, while the focus of concerns refers to the government's surveillance of citizens. On the other hand, the EU privacy rights conceptualization belongs to the personhood realm, which means that one can only license several rights of exploitation on an individual legal position (as it happens with intellectual property rights).

This paper aims to shed light on the Privacy and Data Protection mechanisms related to mobile Health (m-Health) [5], and how to interpret the regulatory requirements of the GDPR correctly.

In this regard, three aspects need to be considered:

1. the EU legal tradition works according to the Civil Law system, which is a framework governed by the so-called "hierarchy of sources". It adopts a top-down approach in which case laws are decided by first interpreting the general principles and general legal provisions to a specific situation. In the EU, the judicial decision (case law) makes no binding precedent, this is the reason why the European regulations – and their norms – are usually general and abstract and requires a specific interpretation to be applied to practical cases. These are, in fact, elements needed for the law to embrace the broadest audience possible (generality), and the broadest situations possible (abstractness). The GDPR works accordingly, and it is "General" precisely because it requires to be implemented by each Member State with national legislations that specify a particular regime (for instance for the digital consent of minors). Therefore, practitioners must read the GDPR together with the national Data Protection law that applies to the single

Commented [A2]: Transposition of EU Regulation into the national domain is not actually the application of the Regulation to a "single case". This is a mechanism stipulated under EU procedural law to show a national way of implementing the Regulation concerned in the respective member states. National data protection laws are general and abstract as well.

case, in order to check if there are specific regimes or additional rules for a particular domain.

2. the GDPR is not a standalone privacy regulation but is part of a legislative body of other Directives and Regulations that compose the EU Data Protection and Privacy regulatory framework [6]. However, The GDPR is a Regulation (and not a Directive), meaning that it is directly self-applicable in every EU Member State (where Directives are not and must be received in the Member State with the issuing of a national law), superseding any conflicting national laws, aside from constitutional fundamental norms or principles.
3. the difference between data and information and consequentially, the difference between data and personal data is important to be distinguished. According to the GDPR[1], *"'personal data' means any information relating to an identified or identifiable natural person ('data subject')"*. Thus, data is an element of information (as a set of specific knowledge), and if it refers to an identified or identifiable natural person, it is personal data. On the contrary, all information that does not entail any link to an identified individual, does not constitute personal data, and as such, does not fall in the GDPR provisions[2] and can be freely processed.

GDPR – General Background

A. Whom the GDPR is related to?

The Regulation binds any data "controller" or "processor" – any public or private company, organization, business or governmental entity (with certain exceptions) that holds, stores, administers or processes any personal data of citizens or residents of the European Union (even

if a non-EU citizen resides in the EU territory)[3]. The difference between the data controller and data processor is that the former establishes the purposes of the data processing, which must drive how personal data are treated and that can be fully disclosed to the data subject. The latter is usually a data controller's proxy, internal or external to its entity, which processes personal data according to the purposes set by the data controller. There is no data processor without data controller, and, if the data processor determines by its own the purposes for the data processing, it must be considered a data co-controller (and shares the consequent liability). The Regulation does not apply to the processing of personal data by a natural person in the course of purely personal activity.

B. What does the GDPR cover?

The Regulation broadly defines "personal data" as: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"[4].

Processing, in turn, "*means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,*

recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

The combination of the two concepts is hugely important, as the EU legislator provided a complete and omni-comprehensive legal regime for every sort of activity that involves the processing of any information in some way related to natural persons. The only exception is the processing by a natural person for personal reasons.

Mobile Health (mHealth)

mHealth is defined as: "*medical and public health practices supported by mobile devices including mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices*"[7].

mHealth apps offer a verity of services [8, 9, 10] and the US National Institute of Mental Health (NIMH) classifies these apps into six categories: Self-management, improving thinking skills, skills-training, supported care, passive symptom tracking, and data collection [11].

Nevertheless, from a Privacy perspective, every single activity listed involves data collection. Indeed, it is the development of new and highly invasive inference techniques of information among single personal data that created the need for more robust legal protection.

GDPR and mHealth

A. "Controllers" and "Processors" in mHealth.

In the field of mHealth, the "controller" is usually a physician or healthcare entity that determines the purpose and the means of the data processing, while the "processor" is the subject that performs the processing activities on behalf of the controller (e.g., the General Practitioner is the controller, and the IT company that collects and analyzes the digital data is the processor).

The Regulation demands that controllers enter into a binding agreement with processors, where the obligations, mechanisms and security safeguards in the agreement will be clearly stated[5]. This practically means that the controller must provide the processors with a specific engagement document (tied to the contract) in which the purposes and limits of the data processing, as well as every relevant information related to it are stated, along with the particular tasks that are requested. If a processor goes beyond the limits defined by the controller, the processor accounts responsible for that breach. If a processor changes the purpose of the processing autonomously or concurs in determining it, the processor will be considered as co-controller and treated accordingly concerning the liability. Finally, the controller has also an obligation to control its processors, for granting the respect of the agreement and, accordingly, if a processor breached the engagement rules and the controller lacks to intervene, both are liable.

B. Personal Data concerning Health.

A critical question that needs to be tackled by practitioners is – what does the GDPR refer to when it indicates *"data concerning health"*?

The implications of the European GDPR in mobile Health

According to the Regulation, *"data concerning health"* is: *"Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"*.

This broad definition of health data distinguishes between three categories: 1) inherently/clearly medical data; 2) raw sensor data that can be used in itself or in combination with other data to make conclusions about health status or risk; 3) outcomes of any sort that are drawn about health status or risk.

Additional clarification can be found under Recital 35 of the Regulation, in which examples for intended data are given: *"Personal data concerning health should include all data pertaining to the health status of an individual, which reveal information relating to his past, current or future physical or mental health status"*.

However, there are still numerous apps falling into the grey area left by the provision, such as those dealing with lifestyle or wellbeing, because they are sets of personal data information that may represent health data. However, the specific classification of these data depends on the analysis of the situation in which the elements that compose the data and the processing must be deconstructed, as follow. Both lifestyle and wellbeing can be broken down into a set of behaviors, such as eating, doing fitness, sleeping, meditating, and so on. If we address fitness, for instance, and the app gathers the heart rate, it is a piece of health information. In contrast, if the app gathers the gyroscope movements of the wearable device (to collect spatial movements) it is a biometric (dynamic) data [21]. Finally, if it collects GPS data, which can be labelled, for instance, as spatial habits, the data processing deals with ordinary personal data. Nevertheless, if these data are collected for health purposes, they should fall into the category of health data.

Commented [A3]: This is a conclusion on which a inquisitive reader would like see more discussion.

In conclusion, it is not only essential to address the type of data but is also important to understand the intended use of the data, as well as the inferential combinations with other data, are also of relevance when determining its classification.

C. Data collecting limitation and data minimization.

The collection of any data must be fair, transparent, and lawful[6] and performed according to legitimate, specific, and explicit purposes[7] on the basis of the legal basis listed by the GDPR[8]. The legitimate purpose calls for an alignment between the necessity of the specific information for the functionality and objectives of the app. In addition, the data's lifecycle should be as minimal as possible, both in quantity and quality, to preserve individuals from unnecessary data processing. If, for instance, the controller's purpose is to measure heart bits, sensors cannot also gather blood pressure data. Furthermore, the principle of limitation and minimization works qualitatively, i.e., in order to fulfil the GDPR requirement, the data processing must take place no longer than the necessary to have an accurate understanding of what was aimed to investigate. In this case a standard duration hart bit rate. Therefore, according to these principles, any personal data retained should also not be stored longer than is necessary[9].

Several key points should be mentioned and addressed:

1. The matter of privacy protection should be addressed right at the initial development of a new app or a new version of an app, as well as at any additional stage of the development. The design process must be addressed and conceived according to these requirements from the very early stage. An app developer should try to anticipate, identify, and prevent invasive events upfront.

Commented [A4]: What if the quality of the measurement of the first requires the collection of the second? That discussion would also be interesting.

Commented [A5]: the legal text would be here more pertinent: "for no longer than is necessary for the purposes for which it was processed."

Commented [A6]: There secure development frameworks and the principle of "privacy by design" that address this conclusion. Reference to these would be useful. Privacy risk assessment (envisaged in GDPR) being performed upfront would also go along with this conclusion.

2. Privacy protection should be the default setting, with components fully integrated into the system: this principle is called "privacy by default". Personal data should be automatically protected, without any additional action required from the user. The least privacy-invasive choice should always be the default one[10]. This means that access to terminal devices sensors or features (camera, microphone, calls, SMS, pictures and so on) must be set up by data controllers only for data necessary according to the purpose of processing.

3. Rights of the data subject - transparency and modalities. First and foremost, a user has a right to access his own personal data, demand corrections and refuse further processing or, alternatively, can enforce the right to restriction or to erasure.

Commented [A7]: Prerequisite for that: "Personal data may only be kept in a form that permits identification of the individual"

D. Transparency

Both controllers and processors must ensure adequate transparency with regard to all practices and technologies[11]. In turn, transparency should embrace every stage and feature related to the data processing, from technological design and architecture to governance and decision-making processes.

Exactly how it has been seen for minimization, transparency is a qualitative concept, i.e., a controller is not required to publish and open every process. On the contrary, the controller must ensure understandability by providing a clear procedure for both allocating the accountability and being able to reconstruct the decision process [12, 13].

E. Security

GDPR protects two legal goods: individuals' personal data and free movement of personal data (data flows). The integrity of the personal data, its availability and confidentiality are crucial, and their protection must be supported by a mechanism of technical, architectural, and organizational measures. Any app should be equipped with a comprehensive security system,

Commented [A8]: The subject matter of protection being free movement sounds not right IMHO. Secure movement maybe.

to protect every stage of the data processing from any accidental or ill-willed destruction, exposure, and other possible shortcomings[12]. Also, it must be considered that those data gathered and processed by controllers are not only individuals' personal data but also an asset for the entity behind the app service. Thus, the rules around the system and architectural security are aimed to ensure protection for both data subjects and data controllers.

Therefore, audit procedures concerning risk assessments should be performed regularly [14], in order to keep updated the data ledgers and track the data flow for ensuring compliance with the regulatory requirements.

Personal data breach

Alongside the preventative measures, the GDPR also deals with the aftermath. When encountering a personal data breach, meaning the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed[13], the Regulation provides a specific guideline of actions to be taken. Amongst the instructions, there is the obligation to inform a Data Protection Authority (DPA) of the breach[14], and the requirement to notify the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons[15]. These notifications must be done without unjustified delay and, however, by 72 hours from the knowledge of the breach. This is an important aspect, as many times can happen that a malware or a hacker "sniffs" the data processing by only monitor the data flow and the controller discover this unlawful activity afterwards. Thus, the obligation starts from the time of the discovery.
However, the notification to data subjects is excluded if the controller adopted technical and organizational measures to avoid the breach (for instance, by anonymizing data) or, after the

discovery of the breach, it adopted adequate measures to fight it back and preserved data subjects' rights.

F. Data gathered from children.

The GDPR provides only a general regime when it comes to children's data (minors, in general). As said, this is one of the cases in which it is vital to read the Regulation together with the national Data Protection law of reference. Parental consent is required for children under the age of sixteen, yet the Member States may determine a lower age of consent (but no younger than thirteen) in their domestic laws[16]. The GDPR does not provide any further requirement. This was intentional, as it is a general regulation and aimed at letting the Member States free to regulate this phenomenon according to their national laws specifically. Indeed, the minors' digital consent overlap and, to a certain extent, conflicts with the general Civil Law system rules about legal capacity, which, usually, is set up with the majority age at 18 years old (depending on countries). It may create abuses and grey areas [15]. Thus, when an app focuses on providing services to minors, it must address the issue looking for the effective place in which minors will use the service, and their data will be gathered. That place will determine the national law applicable. If it lacks to establish precise requirements and instructions for minors' data processing, the controller must inform its activity according to the general principles. This means that the accountability principles work to fill the regulatory gap by inducing the controller to provide a correspondent level of security and compliance. Thus, for minors, controllers must adopt higher standards of protection. To put this in practical terms, mApps must determine in advance whether they will potentially gather minors' data, where they would do so, and align their activity to the national requirements. In general, the mApp will have to determine the age (identity) of the minor in order to check the limits for a valid

minor's consent and, on the contrary case, designing an effective tool to require parents' consent (such as for instance, SMS, ID number and so on).

G. Secondary purposes

Secondary purposes are those further purposes that might arise during data processing already started. For instance, if an app collects heart rates for the purpose of monitoring health status and, afterwards, the controller wants to use these data for inferring other information such as stress periods and so on, it must disclose to data subjects this secondary purpose and gather their further consent [16]. Thus, when processing data for secondary purposes, any secondary purpose must agree with the original purpose, or else complementary consent will be required. Furthermore, it is not possible for a controller to bypass these requirements by providing data subjects in advance with an omni-comprehensive information form that entails every potential processing purpose. This is the reason why Big Data related to personal data are intrinsically unlawful according to GDPR general principles. Indeed, the Big Data concept itself grounds on the idea of a vast mass of raw data collected and stored for unforeseeable purposes and processed whenever it will be necessary for emerging and contingent scopes [17]. With that being said, additional processing for the purpose of public interest, scientific or historical research or statistics, is considered fitting with the original purpose, as long as it is compatible with state or union laws[17]. This, however, does not release the controller from the duties of information, as stated in articles 13 and 14. Moreover, these purposes are typically excluded for those players who already perform business-oriented data processing.

H. Third party

Some cases require a controller/processor to communicate personal data to a third-party recipient for processing operations. In such cases, the developer has to engage in a legally binding agreement with the third party, and the user must be informed prior to the disclosure of the data [18]. The binding agreement involves an engagement letter and, therefore, the third party becomes a processor itself. Data subjects must be informed in advance, but the law requires only to disclose in the consent form the categories of these third parties, providing the data subjects with the instructions to find elsewhere (typically in a web page) the full list of the actual processors. This expedient aims to facilitating the controller's activity, as third parties relationships may change during the data processing, and this dynamic list avoid it to update the consent form every time. Also note that when a processor quits for whatever reasons from its engagement with the controller, it must delete every personal data processed (usually according to the engagement letter and the binding agreement), aside from those strictly necessary or required by the law (for tax issues, for instance).

I. Transfer of data

Other cases require the transfer of data outside of the EU or EEA (onto a third country or an international organization). In such cases, the transfer of data must rely on a legal authorization[19] (such decisions of the European Commission via national Authorities, Binding Corporate Rules or international agreements)[20] [18, 19]. It is an open treaty to which private companies or entire States can adhere, ensuring the respecting of those written principles and rules that refer to the GDPR and the complete EU Privacy and Data Protection legal regime. It should be noted that, in lack of any out of the ordinary circumstances, the Regulation prohibits the transfer of personal data to countries outside of the EU, unless they offer an adequate level of protection as determined by the European Commission[21], which

means they adhere to the Privacy Shield agreement. However, a recent decision from the European Court of Justice[22] of the so-called "Schrems II" case has invalidated EU-US Data Protection Shield, which, therefore, cannot be used anymore as a legal basis to transfer personal data outside the European Union. For this reason, the European Data Protection Board (EDPB) has issued a series of FAQs to provide first guidance during the vacancy of a valid regulatory framework to transfer personal data abroad[23]. However, the binding-corporate rules (BCR) and standard contractual clauses (SCC) still remain valid and can be used lawfully[24].

J. Research activities

The GDPR recognizes the unique attributes of research (defined as all activities of public and private entities alike)[25]. Thus, it allows that some requirements, such as those concerning secondary processing and using sensitive data, can be forsaken as long as appropriate safeguards are implemented[26]. Furthermore, in some exceptions, the Regulation allows researchers to access data without consent[27] and override requests to delete data[28]. However, this leniency is only acceptable when it is deemed necessary for the fulfilment of the research purposes and only if allowing data subjects to exercise their rights likely would seriously impair the achievement of the specific purposes[29]. Also, data subjects must be informed according to the general requirements and maintain the right to object the processing for justified reasons. However, a Data Protection Authority (DPA) or a judge might negate this objection on the ground of the balance between opposite rights, public interest purposes or other justified legal motivations. Furthermore, note that the data controller cannot claim research and historical purposes when performing other business activities connected with the same data processing. Thus, secondary processing is allowed only when the entity is a third party without business or profit aims.

The safeguards that are being expected from researchers are those that ensure adherence to good practice rules, a valid approval from a Research Ethics Committee, and data minimization[30] and anonymization (according to the Regulation, anonymity can only be achieved when the data cannot be identified by any means reasonably likely to be used either by the controller or by another person)[31] where possible. Nevertheless, this is another case in which the GDPR must be integrated with the national Privacy law, which might provide some further requirement or specification.

K. Data Subject's Consent

One of the main emphasizes of the GDPR is the procedure to obtain valid consent. If the legal basis selected for the data processing is the individual's consent, any data processing must be based on the data subject's free, informed, unambiguous and specific consent. When it comes to processing health data the data subjects' consent must be gathered explicitly (opt-in) for that purpose [16, 20]. The GDPR considers the rule of consent as the preeminent legal basis for the data processing, according to the disposal of article 8 of the EUCFR. Still, others are in place, such as legitimate interest.

The wording of the consent form must be manifested in a clear, and unequivocal way. The purpose for which the data is being collected must be directly pointed out, along with all the requirements provided by the GDPR in terms of transparent data processing [32].

Moreover, the user has both the right to erasure, i.e. the right to be "forgotten", and to opposition (each according to certain limits). This means that in case the data subject withdraws their consent, any of their prior personal information must be completely deleted[33]. Data subjects can also claim the right to access[34] the personal data which the controller processes, as well as the right to portability[35] about the data that the data subjects themselves have provided to the data controller.

Conclusion

As the field of mHealth keeps on growing, it provides new opportunities along with new challenges. One of the most important one is how to process personal data in a compliant and fair way, and accordingly, how to protect individuals and their privacy. The GDPR provides an acceptable balance between the potential benefits and the emerging risks while merging digital technologies into the medical field. The paper addresses the practitioners' need for a clear understanding of the regulatory landscape, concepts and the requirements of data collection and processing under GDPR.

The authors also emphasis the practical implications, research, consent validity and secondary analyses for research purposes.

A better understanding of the GDPR and its conceptual legal framework will help those medical stakeholders who are planning to embark on adapting mobile technologies in their research. and\or practice

Disclosure statement

Funding: Not applicable

Conflicts of interest: The authors declare no conflict of interest.

Availability of data and material: Not applicable

Code availability: Not applicable

Authors' contributions: All authors participated in writing the first draft and editing the MS.

Ethics approval: Not applicable

Consent to participate: Not applicable.

Consent for publication: All authors agree with publication.

Endnotes

GDPR Article 4(1)
[2] GDPR Article 2
[3] GDPR Articles 3, and 4
[4] GDPR, Articles 4
[5] GDPR, Recital 80; and Article 28(3)
[6] GDPR Article 5(a)
[7] GDPR Article 5(b)
[8] GDPR Article 6
[9] GDPR, Article 5(b)
[10] GDPR, Article 25
[11] GDPR, Articles 18, 19, and 21
[12] GDPR, Article 32
[13] GDPR, Article 4(12)
[14] GDPR, Article 33

[15] GDPR, Article 34
[16] GDPR, Article 8
[17] GDPR, Articles 5(b),13(3),14(4), and 89
[8] GDPR, Article 4(9) and 4(10)
[19] GDPR, Articles 44 and 45
[20] GDPR, Articles 4(20), 46, 47 and 48.
[21] GDPR, Article 45(1)
[22] Decision on Judgement case C-311/2018 (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems) that has invalidated the Decision 2016/1250 on adequacy of the protection provided by the EU-US Data Protection Shield. See https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (last accessed on 30 of July, 2020).
[23] EDPB FAQ on CJEU judgment C-311/18 (Schrems II): See https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_it (last accessed on 30 of July, 2020).
[24] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en for more detailed information. (last accessed on 30 of July, 2020).
[25] GDPR, Recital 159
[26] GDPR, Recital 50; and Article 6(4)
[27] GDPR, Recitals 47,157; and Article 6(1)(f)
[28] GDPR, Articles 5(1)(b),17(3)(d), 21(6), and89(2)
[29] GDPR, Article 89(2)
[30] GDPR, Articles 5(c),89(1)
[3] GDPR, Recital 26, and Articles 4(3)(b) and89(1)
[32] GDPR, Article 7
[33] GDPR, Article 17
[34] GDPR Article 16
[35] GDPR Article 20

Bibliography

[1] European Union, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), which was approved and come into force on 27 April 2016. [Hereinafter: "GDPR"].

[2] European Data Protection Supervisor (EDPS) Opinion No. 3/2018 on online manipulation and personal data.

[3] European Parliament, Directorate General for Internal Policies, A comparison between US and EU Data Protection legislation for Law enforcement, 2015.

[4] Paul M. Schwartz, The EU-US Privacy collision: a turn to Institutions and Procedures, Harvard Law Review, Vol. 126, No. 7 (MAY 2013), pp. 1966-2009

[5] EDPS, Opinion 1/2015 on Mobile Health, Reconciling technological innovation with data protection.

[6] European Data Protection Supervisor, Executive summary of the opinion of the European Data Protection Supervisor on the EU-US Privacy Shield draft adequacy decision, (2016/C 257/05).

[7] World Health Organization Report (2011). mHealth: New horizons for health through mobile technologies. *World Health Organization*, *64*(7), 66-71.

[8] European Data Protection Supervisor, Opinion 1/2015 on Mobile Health, Reconciling technological innovation with data protection.

[9] European Data Protection Supervisor, Opinion of the on the Communication from the Commission on 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century'. 2013

[10] Article 29 Working Party, 00461/13/EN WP 202, Opinion 02/2013 on apps on smart devices, Adopted on 27 February 2013.

[11] The National Institute of Mental Health (2017). Technology and the Future of Mental Health Treatment. Retrieved from: https://www.nimh.nih.gov/health/topics/technology-and-the-future-of-mental-health-treatment/index.shtml

[12] Article 29 Working Party, 17/EN WP260 rev.01, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018.

[13] Mantelero, A. 2014. Social Control, Transparency, and Participation in the Big Data World. Journal of Internet Law, April: 23-29

[14] Article 29 Working Party, 17/EN WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017.

[15] N. Vlajic, M. El Masri, G. M. Riva, M. Barry, D. Doran, Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR. ACM CCS MPS Workshop: Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, 2018.

[16] Article 29 Working Party, 17/EN WP259 rev.01, Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, As last Revised and Adopted on 10 April 2018.

[17] European Data Protection Supervisor, Executive Summary of the Opinion of the European Data Protection Supervisor on effective enforcement in digital society economy, (2016/C 463/09).

[18] Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, (2009/C 128/03), Official Journal of the European Union, C 128/20, 6.6.2009.

[19] European Data Protection Supervisor, Executive summary of the opinion of the European Data Protection Supervisor on the EU-US Privacy Shield draft adequacy decision, (2016/C 257/05).

[20] Irish Data Protection Commissioner, Data Protection Guidelines on research in the Health Sector, 2007.

[21] Gianluigi M. Riva, Metadata, Semantic-data and their protection: legal nature and issues under the GDPR and the E-Privacy draft Regulation, In 2018 Amsterdam Privacy Conference Proceedings.