MEDINFO 2021: One World, One Health – Global Partnership for Digital Innovation
P. Otero et al. (Eds.)

doi:10.3233/SHTI220066

General Data Protection Regulation (GDPR) Toolkit for Digital Health

Rada Hussein[a], Daniela Wurhofer[a], Eva-Maria Strumegger[a,b], Andreas Stainer-Hochgatterer[a], Stefan Tino Kulnik[a], Rik Crutzen[c], and Josef Niebauer[a,d]

[a] Ludwig Boltzmann Institute for Digital Health and Prevention, Salzburg, Austria,
[b] Salzburg University of Applied Sciences, Salzburg, Austria,
[c] CAPHRI Department of Health Promotion, Maastricht University, Maastricht, The Netherlands,
[d] University Institute of Sports Medicine, Prevention and Rehabilitation,
Paracelsus Medical University, Salzburg, Austria

Abstract

The General Data Protection Regulation (GDPR) entered into force on May 25, 2018. Compliance with GDPR is especially relevant to the Digital Health (DH) domain, as it is common to process highly sensitive personal data regarding a person's health. However, GDPR compliance is a very challenging process since it requires implementing several technical and organizational measures to maintain compliance.

With the aim to facilitate this process, we reviewed the published best practices in GDPR compliance. Then, we customized the findings to fit into the DH domain and created a toolkit for GDPR implementation and compliance. The Activity Planning Tool (APT) is provided as an example of how this toolkit could be utilized in new application development in mobile health in Austria. In the case of our APT, the toolkit was very helpful in integrating the GDPR technical requirements in addition to creating the corresponding compliance impact assessment, processing agreements, privacy policy, data flowcharts, and compliance checklists.

Keywords:

Consent, Data Protection, Digital Health

Introduction

With the enforcement of the European Union (EU)-General Data Protection Regulation (GDPR) in 2018 [1], data privacy and data security compliance became two essential components for the data protection strategy of any organization processing personal data in the EU. GDPR also introduced several new compliance obligations, such as more explicit informed consent, the right to be forgotten, the mandatory assignment of a Data Protection Officer (DPO) for certain processing situations, the obligation to report the data breach to data protection authorities within 72 hours of having become aware of it, in addition to a stricter sanctioning regime for non-compliance [1].

In the Digital Health (DH) domain, DH apps must be able to protect highly sensitive personal data (including medical, wellness, lifestyle, and behavior data) in accordance with the GDPR requirements. These sensitive personal data are mainly considered as a GDPR special category concerning health. Thus, DH researchers, companies, clinicians, and others need to spend extra efforts in understanding, implementing, and maintaining compliance with the GDPR organizational and technical requirements [2].

There are numerous publications on GDPR best practices from different domains available. These resources are mainly published by EU projects [3] and member state informatics organizations, such as the French Data Protection Authority [4]. Additionally, there are state-of-the-art publications on implementing the GDPR technical requirements, including data encryption, authorization, and access control, and consent management. Valuable guidance in this regard is provided by international consultancy companies and DH industry [5-7].

However, it remains challenging to define precisely a roadmap for GDPR implementation and compliance in DH, covering both legal and technical aspects. This paper aims to introduce a toolkit for GDPR implementation and compliance in DH at the institutional level at the Ludwig Boltzmann Institute for Digital Health and Prevention (LBI-DHP). It also provides a clear roadmap on how to develop our DH Apps in compliance with GDPR. Our DH app, the Activity Planning Tool (APT), is provided as an example to demonstrate the usability of the toolkit during the APT design and development phases.

Methods

A comprehensive narrative literature review was conducted to create the toolkit. The criteria of searching were utilized while searching several databases, including scientific portals and journals (e.g., PubMed, Google Scholar, etc.), organization portals (European Commission, Integrating the Healthcare Enterprise, Information Commissioner's Office, National Commission on Informatics and Liberty, etc.), consultation agencies, and commercial companies' resources (Deloitte, Chino.io, etc.). The search criteria also targeted materials published in English from 2017 till February 2020. Search terms selected for the literature search include digital health, mobile health (mHealth), eHealth, GDPR implementation strategy, compliance checklists, and best practices using Boolean operators (OR/AND).

More than 300 publications were retrieved covering a wide-scale of scientific literature on GDPR compliance and implementation guides. All publications were reviewed and qualitatively evaluated by the authors and the LBI-DHP principal investigators and co-investigators. The selected documents were customized to the DH domain through:

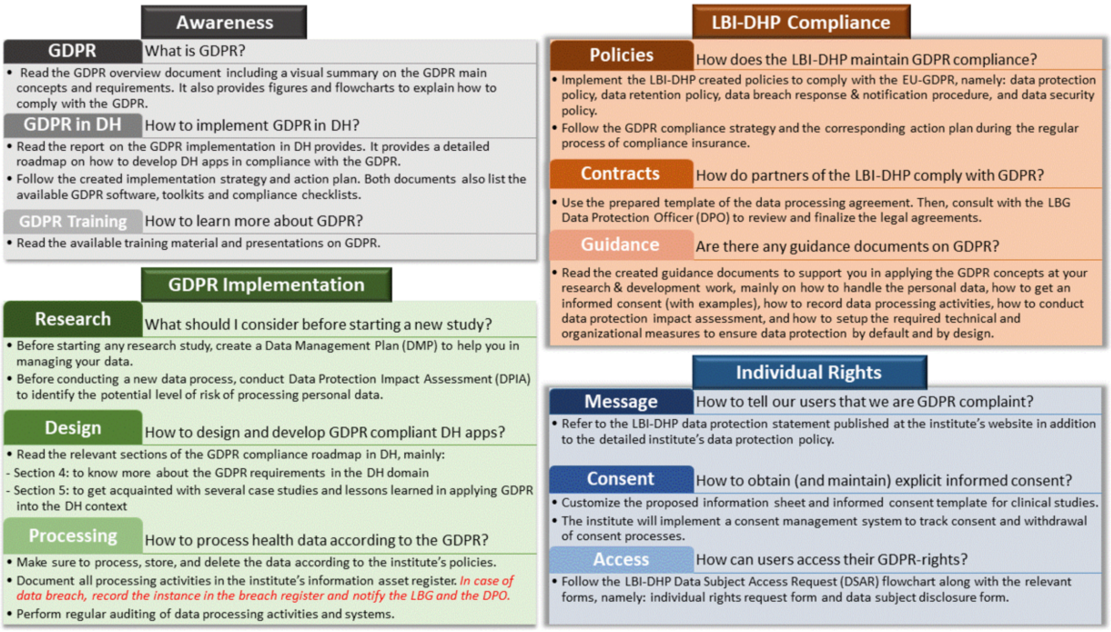
The customized documents were discussed with the Ludwig Boltzmann Gesellschaft (LBG) legal department and reviewed by the LBG-DPO.

Finally, the toolkit was created comprising the customized documents and applied to the APT for assessment of its practicality.

Results

The created GDPR toolkit for DH consists of four categories, as summarized in Figure 1.

- the necessity to be published on the organization website.
- Incorporating the best practices in mHealth, for example, the privacy framework for mHealth application [8],
- Addressing the state of the art in different data security aspects as well as new concepts like “security as service” in the technical roadmap document,



Awareness

GDPR What is GDPR?

- Read the GDPR overview document including a visual summary on the GDPR main concepts and requirements. It also provides figures and flowcharts to explain how to comply with the GDPR.

GDPR in DH How to implement GDPR in DH?

- Read the report on the GDPR implementation in DH provides. It provides a detailed roadmap on how to develop DH apps in compliance with the GDPR.
- Follow the created implementation strategy and action plan. Both documents also list the available GDPR software, toolkits and compliance checklists.

GDPR Training How to learn more about GDPR?

- Read the available training material and presentations on GDPR.

GDPR Implementation

Research What should I consider before starting a new study?

- Before starting any research study, create a Data Management Plan (DMP) to help you in managing your data.
- Before conducting a new data process, conduct Data Protection Impact Assessment (DPIA) to identify the potential level of risk of processing personal data.

Design How to design and develop GDPR compliant DH apps?

- Read the relevant sections of the GDPR compliance roadmap in DH, mainly:

- Section 4: to know more about the GDPR requirements in the DH domain
- Section 5: to get acquainted with several case studies and lessons learned in applying GDPR into the DH context

Processing How to process health data according to the GDPR?

- Make sure to process, store, and delete the data according to the institute’s policies.
- Document all processing activities in the institute’s information asset register. *In case of data breach, record the instance in the breach register and notify the LBG and the DPO.*
- Perform regular auditing of data processing activities and systems.

LBI-DHP Compliance

Policies How does the LBI-DHP maintain GDPR compliance?

- Implement the LBI-DHP created policies to comply with the EU-GDPR, namely: data protection policy, data retention policy, data breach response & notification procedure, and data security policy.
- Follow the GDPR compliance strategy and the corresponding action plan during the regular process of compliance insurance.

Contracts How do partners of the LBI-DHP comply with GDPR?

- Use the prepared template of the data processing agreement. Then, consult with the LBG Data Protection Officer (DPO) to review and finalize the legal agreements.

Guidance Are there any guidance documents on GDPR?

- Read the created guidance documents to support you in applying the GDPR concepts at your research & development work, mainly on how to handle the personal data, how to get an informed consent (with examples), how to record data processing activities, how to conduct data protection impact assessment, and how to setup the required technical and organizational measures to ensure data protection by default and by design.

Individual Rights

Message How to tell our users that we are GDPR complaint?

- Refer to the LBI-DHP data protection statement published at the institute’s website in addition to the detailed institute’s data protection policy.

Consent How to obtain (and maintain) explicit informed consent?

- Customize the proposed information sheet and informed consent template for clinical studies.
- The institute will implement a consent management system to track consent and withdrawal of consent processes.

Access How can users access their GDPR-rights?

- Follow the LBI-DHP Data Subject Access Request (DSAR) flowchart along with the relevant forms, namely: individual rights request form and data subject disclosure form.

Figure 1- GDPR toolkit summary (an overview in the form of Q&A to guide the institute’s team members)

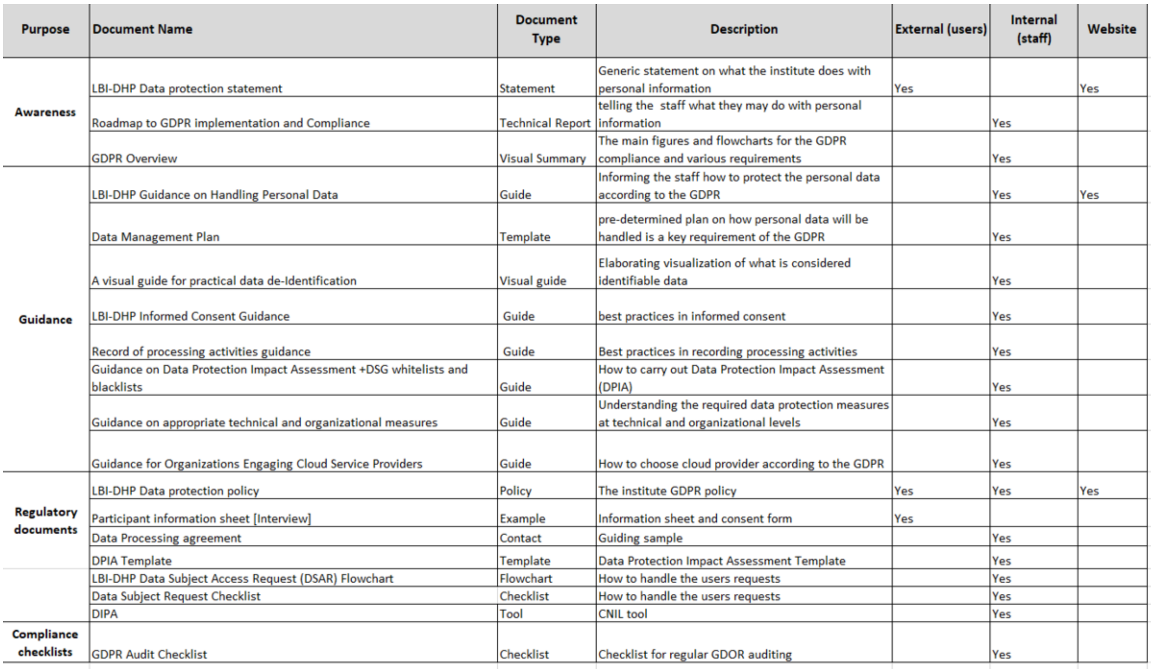
In order to provide the staff of our Ludwig Boltzmann Institute of Digital Health and Prevention (LBI-DHP) with a clear understanding on how/what/when/where to use the toolkit, the Questions and Answers (Q&A) format has been used.

Accordingly, the toolkit provides the required GDPR templates and materials as follows:

1. **Awareness:** GDPR tutorials and training materials
2. **Organizational compliance:** a regulatory framework including policies, contractual templates, and checklists for institutional GDPR compliance
3. **GDPR implementation in DH:** a detailed roadmap for the GDPR technical implementation and compliance in DH, including compliance strategy and action plan.
4. **Practicing GDPR individual rights:** guidelines, user forms, and flowcharts for supporting the user of DH apps.

Table1 shows the GDPR toolkit and lists some of the created documents indicating the following:

- the purpose of the document,
- document name,
- document type,
- brief description of the document,
- type of use (internal or external), and
- Specifying and categorizing the health and fitness data types that will be generally processed within DH apps, and
- Complying the toolkit with the GDPR aspects of the Austrian laws.



Purpose	Document Name	Document Type	Description	External (users)	Internal (staff)	Website
Awareness	LBI-DHP Data protection statement	Statement	Generic statement on what the institute does with personal information	Yes		Yes
	Roadmap to GDPR implementation and Compliance	Technical Report	telling the staff what they may do with personal information		Yes	
	GDPR Overview	Visual Summary	The main figures and flowcharts for the GDPR compliance and various requirements		Yes	
Guidance	LBI-DHP Guidance on Handling Personal Data	Guide	Informing the staff how to protect the personal data according to the GDPR		Yes	Yes
	Data Management Plan	Template	pre-determined plan on how personal data will be handled is a key requirement of the GDPR		Yes	
	A visual guide for practical data de-Identification	Visual guide	Elaborating visualization of what is considered identifiable data		Yes	
	LBI-DHP Informed Consent Guidance	Guide	best practices in informed consent		Yes	
	Record of processing activities guidance	Guide	Best practices in recording processing activities		Yes	
	Guidance on Data Protection Impact Assessment +DSG whitelists and blacklists	Guide	How to carry out Data Protection Impact Assessment (DPIA)		Yes	
	Guidance on appropriate technical and organizational measures	Guide	Understanding the required data protection measures at technical and organizational levels		Yes	
	Guidance for Organizations Engaging Cloud Service Providers	Guide	How to choose cloud provider according to the GDPR		Yes	
Regulatory documents	LBI-DHP Data protection policy	Policy	The institute GDPR policy	Yes	Yes	Yes
	Participant information sheet [Interview]	Example	Information sheet and consent form	Yes		
	Data Processing agreement	Contact	Guiding sample		Yes	
	DPIA Template	Template	Data Protection Impact Assessment Template		Yes	
	LBI-DHP Data Subject Access Request (DSAR) Flowchart	Flowchart	How to handle the users requests		Yes	
	Data Subject Request Checklist	Checklist	How to handle the users requests		Yes	
	DIPA	Tool	CNIL tool		Yes	
Compliance checklists	GDPR Audit Checklist	Checklist	Checklist for regular GDOR auditing		Yes	

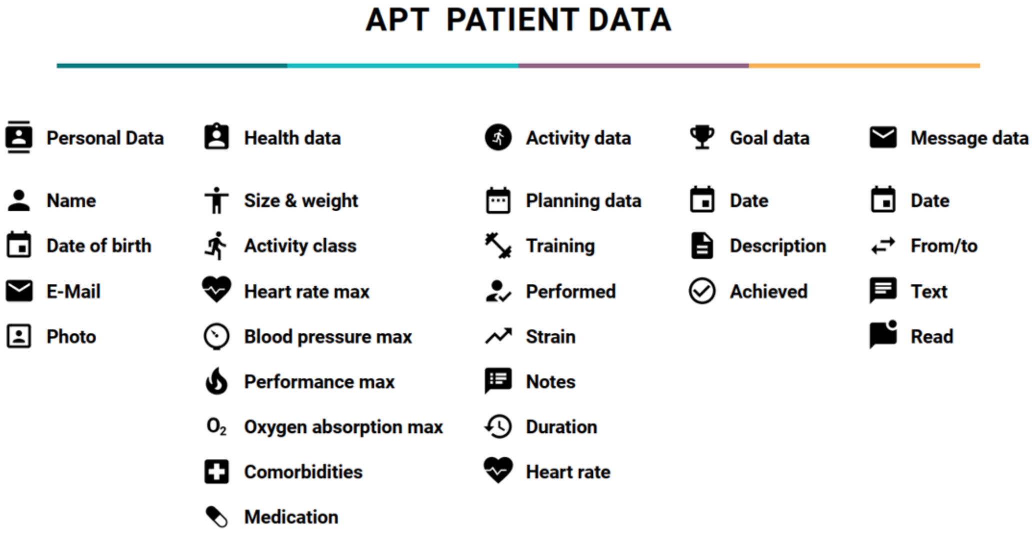


Figure 2- Visualization of APT data types using icons

The toolkit was utilized in the APT to develop an app that is in compliance with GDPR. The APT is currently used in our outpatient cardiac rehabilitation department to support patients in adhering to their personalized exercise prescription and activity planning.

The toolkit facilitated the incorporation of the GDPR requirements following the toolkit guidance and recommendation, as follows:

- At the institutional level, the awareness and training material provided the APT development team with a better understanding of GDPR requirements before developing the app. For instance, the APT team was able to create the required templates and checklists for reporting and assessing the GDPR compliance of APT during the early conception and ideation phase of the project. This facilitated the consideration of GDPR aspects in the early beginning of APT analysis and prototyping phases, covering the GDPR concepts of data minimization, privacy by default, and privacy by design. After the development phase, the development team finalized the evaluation report on the APT GDPR integrated service in terms of functionality and lessons learned.
- At the technical level, the toolkit provided a clear roadmap and recommendation for fulfilling the APT's GDPR technical requirements. We integrated commercial Application Programming Interfaces (APIs) for data encryption (at record level), consent management, user identity and authentication, access control policies, audit logs, and encrypted backups. Besides, the roadmap highlighted the mandate of providing visual interfaces for clear communication with the user to provide explicit informed consent - based on the recommendations of translating GDPR into mHealth practice [9]. Thus, we utilized visualization and icons in the APT ePrivacy Policy to identify the data collected and processed by APT, as shown in Figure 2. For the APT app, the consent process has two stages. The first one is verbal to start the APT registration. The second one is for getting informed consent using iconized health data visualization. Most of the icons were taken from the Material Design Icons Collection (https://materialdesignicons.com/). Only a few icons (e.g., for maximal oxygen consumption and maximal blood pressure) were added.
- At the implementation level, within a new project such as the APT described in this paper, the toolkit facilitated the conduction of the Data Protection Impact Assessment (DPIA) of the APT. We utilized the customized DPIA template and associated guidelines. It also guided the creation of DPIA supported documents, such as the APT dataflow and the APT sign-up process flowchart (see Figure 3).

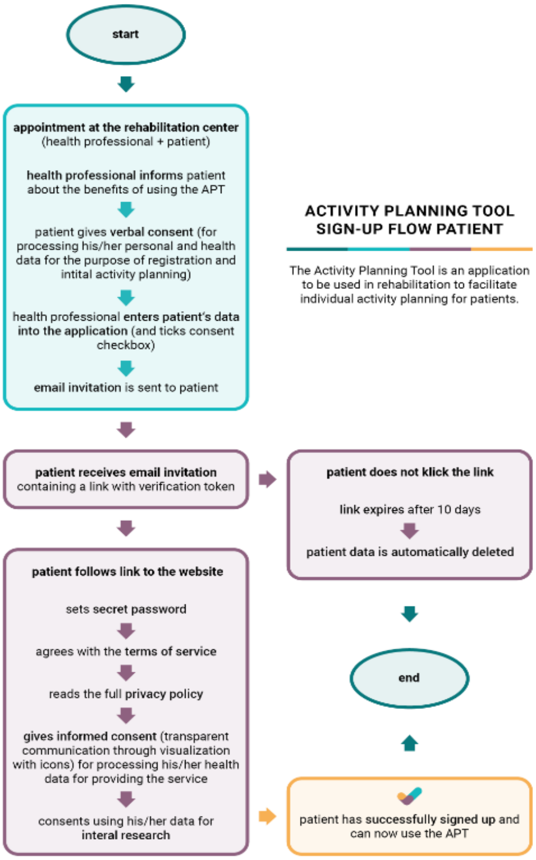

start
appointment at the rehabilitation center
(health professional + patient)
health professional informs patient about the benefits of using the APT
patient gives verbal consent (for processing his/her personal and health data for the purpose of registration and intital activity planning)
health professional enters patient's data into the application (and ticks consent checkbox)
email invitation is sent to patient
ACTIVITY PLANNING TOOL
SIGN-UP FLOW PATIENT
The Activity Planning Tool is an application to be used in rehabilitation to facilitate individual activity planning for patients.
patient receives email invitation containing a link with verification token
patient does not klick the link
link expires after 10 days
patient data is automatically deleted
patient follows link to the website
sets secret password
agrees with the terms of service
reads the full privacy policy
gives informed consent (transparent communication through visualization with icons) for processing his/her health data for providing the service
consents using his/her data for interal research
end
patient has successfully signed up and can now use the APT

Figure 3- APT sign-up process

Discussion

GDPR has become necessary for everyday research practices, especially in DH. Consequently, it is essential to be prepared for all GDPR aspects in advance. Aspects like obtaining informed consent, data minimization, data anonymization, and open science have to be considered in time in order to help facilitate the researcher's everyday practice [10].

The GDPR as regulation requires implementation into the national laws by the EU's Member States, and this process will differ between the Member States. For instance, in Austria, we comply with GDPR and the Austrian Data Protection Act (DSG). This also was reflected while conducting the DPIA for the APT. The preliminary risk analysis had to be conducted according to whitelists and blacklists identified by Austrian law. Therefore, DH researchers should consider the different GDPR implementation in the EU when considering wide-scale deployments of DH apps within Europe. The toolkit provides a generic set of the required GDPR documents that can be easily customized into different legal contexts.

The GDPR toolkit provided a customized set of policies, guidance, templates, and checklists for GDPR implementation and compliance in DH. In the future, it would be very beneficial to develop a platform for customizing, handling, and maintaining this GDPR regulatory framework in a digital format. In this way, it will be much easier to control and share the GDPR required documents.

Conclusions

GDPR compliance in DH requires proper integration between the legal and technical aspects. The GDPR requirements cover physical (i.e., hardware, cloud architecture, etc.), technological (i.e., software and apps development), and organizational (i.e., legal and assessments) requirements.

The described GDPR toolkit facilitated and accelerated the GDPR implementation and compliance processes in the DH domain. The provided example of applying the toolkit on our APT app showed how the toolkit supported GDPR compliance from the early stage of the app design and development.

Acknowledgments

This GDPR compliance activity was conducted within the scope of the Co-production of home-based digital support for cardiac patients (CODIS) project, funded by the Ludwig Boltzmann Gesellschaft (LBG) Open Innovation in Science (OIS) Center under the "Research Enrichment Fund: COVID-19 Support Measures".

The authors would like to thank Dr. Bernd Schauer, the LBG DPO, for reviewing the toolkit documents, providing legal customization to the Austrian laws, and supporting the APT GDPR activities.

Special thanks also extended to Mag. Andreas Egger, Dr. Barbara Mayr, Dr. Bernhard Reich, and Dr. Mahdi Sareban from the University Institute of Sports Medicine, Prevention and Rehabilitation for their participation in APT co-design workshops and GDPR implementation activities.

References

[1] EU data protection rules [Internet]. European Commission - European Commission. [cited 2021 April 9]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en.

[2] Mondschein CF, Monda C. The EU's General Data Protection Regulation (GDPR) in a Research Context. In: Kubben P, Dumontier M, Dekker A, editors. Fundamentals of Clinical Data Science [Internet]. Cham (CH): Springer; 2019 [cited 2021 April 10]. Available from: https://pubmed.ncbi.nlm.nih.gov/31314241/

[3] General Data Protection Regulation (GDPR) Compliance Guidelines [Internet]. GDPR.eu. [cited 2021 April 9]. Available from: https://gdpr.eu/

[4] GDPR Guide [Internet]. French Data Protection Authority (CNIL). [cited 2021 April 9]. Available from: https://www.cnil.fr/en/home.

[5] Understanding the General Data Protection Regulation (GDPR). Deloitte Malta risk advisory; 2018.

[6] eBooks for health and medical app security [Internet]. [cited 2021 April 9]. Available from: https://www.chino.io/blog/healthcare-app-development-resources/

[7] GDPR Checklist - Cloud Security Checklist for GDPR Compliance [Internet]. [cited 2021 April 9]. Available from: https://tresorit.com/gdpr/gdpr-checklist

[8] Mustafa U, Pflugel E, Philip N. A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). 2019. p. 1–9.

[9] Muchagata J, Ferreira A. Translating GDPR into the mHealth practice. In: 2018 International Carnahan Conference on Security Technology (ICCST). 2018. p. 1–5.

[10] Crutzen R, Ygram Peters G-J, Mondschein C. Why and how we should care about the General Data Protection Regulation. Psychol Health. 2019;34(11):1347–57.

Address for correspondence

Rada Hussein, rada.hussein@dhp.lbg.ac.at,
Ludwig Boltzmann Institute for Digital Health and Prevention,
Lindhofstrasse 22, 5020 Salzburg, Austria.