Privacy in Mobile Health Applications for Breast Cancer Patients

Jaime Benjumea, Enrique Dorronzoro, Jorge Ropero, Octavio Rivera-Romero, Alejandro Carrasco

Universidad de Sevilla
Department of Electronic Technology
Seville, Spain
benjumea@dte.us.es, enriquedz@dte.us.es, jropero@us.es, orivera@us.es, acarrasco@us.es

Abstract—**Privacy is a major concern for breast cancer patients. When patients use mobile health applications (mHealth apps), many sensitive data are handled by the application developers. General Data Protection Regulation (GDPR) arises as a solution to privacy issues. In this paper, we analyze the privacy policy of a sample of mHealth apps for breast cancer patients, developing a scale to check if GDPR is complied. Despite privacy is a key factor in the adoption of the use of mHealth apps, the low level of compliance with the GDPR of the analyzed applications was quite surprising. Thus, application developers must be concerned about this matter.**

Keywords: breast cancer, privacy, GDPR; mHealth; mobile applications.

I. Introduction

Breast cancer (BC) is the most common cancer in women [1,2]. Nowadays, the early BC detection and advancements in treatments have resulted in an increased survivorship [3-5]. However, BC survivors live with the effects of those treatments and possible complications [6], requiring them to be proactive in the care of their health. They must address medical and psychological concerns and needs in the post-treatment period [7]. Technological solutions may provide effective tools for health education, self-monitoring, communication, etc., supporting them in the self-management of those survivorship issues.

Connected Health, where these solutions may be included, is a technology-enabled healthcare delivery model aimed to maximize healthcare resources [8]. Mobile Health (mHealth), a subdomain of Connected Health, is defined as the delivery of healthcare or health related services using portable devices [9]. Among portable devices, smartphones are particularly interesting due to their increased global use, ubiquity, high cost-effectiveness, and capabilities, such as tracking users' behaviors and providing them real-time feedback. The use of mobile health applications (mHealth apps) for health and well-being promotion has increased rapidly in recent years [10]. In the case of BC, Giunti et al. reviewed BC mHealth apps available in the leading smartphones app stores (Apple Store and Google Play) finding 454 mHealth apps intended for patients [11]. 114 of those mHealth apps were focused on disease management.

Common features included in those BC mHealth apps for disease management such as activity tracking, health diaries, or patient reported outcomes, require patient to enter data into the app. Some of those mHealth apps even allow patients to share their data with others. Most of BC patients are willing to share their data with a healthcare team, but they may be reluctant to share them with others [12-14]. Data privacy is a common concern among patients regarding the use of mHealth apps to self-manage their health [15, 16]. Privacy and security of user information contained in the mHealth apps has been reported as a relevant issue in the evaluation of their safety and quality [17].

In this paper, we assess the privacy policies of a sample of BC mHealth apps. With this aim, we introduce a novel scale for assessing privacy. The scale is based on the General Data Protection Regulation (GDPR), applicable since 2018 across the European Union (EU). Our scale defines a score for every mHealth app based on several GDPR items that must be complied. We analyzed a sample of 9 mHealth apps for BC self-management, applying our novel privacy assessment scale.

The paper is organized as follows. Section 2 deals with the legal and technical background. Legal background includes some GDPR features and definitions that are useful for our research. Research background presents a brief description of related work previously published in both general and eHealth privacy policy assessments. Section 3 describes the privacy scale designed based on its privacy policy and we define the screening method for selection of the BC mHealth apps. In Section 4, we show the main results of our study. Finally, Section 5 shows our main conclusions about the analysis.

II. Background

A. *Legal background*

Regulation 2016/679 of the European Parliament and of the Council, also known as General Data Protection Regulation (GDPR) [18], was published in the Official Journal of the European Union on 27 April 2016. GDPR is applicable to all member states since 25 May 2018.

GDPR harmonizes the legislation across the whole European Union. It is an 88-page document and contains 99 articles. Some of the most important features are the following:

- **Harmonization**: It applies to all Member States directly, without needing to be translated it into a national law.
- **It applies to all the establishments in the EU**, controllers or processors – see definitions below -, even if processing occurs outside the EU. (Article 3.1).
- **It applies to EU people's data**, even if the controller or processor is not from the EU, but it offers goods or services to people in the EU (Article 3.2) or it monitors users' behaviors.
- **Accountability**: the controller shall be responsible for the compliance with GDPR. GDPR allows a controller to adhere to codes of conduct or certification, so that the compliance can be easily verified. (Article 5.2)
- **Coercion**: Coercive measures are stronger. A supervisory authority may fine the controller with up to 20,000,000 EUR. Also, a supervisory authority may adopt provisional measures in case there is an urgent need to act to protect data subjects' rights. (Articles 83 and 66)

Moreover, GDPR defines some important concepts for regulation. Most definitions can be found in article 4, except otherwise indicated. We are using the following in this paper:

- **Data subject**: identified or identifiable natural person whose personal data are being processed. Any data that makes someone identified or identifiable is personal data, according to GDPR.
- **Controller**: "the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data"
- **Processor**: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"
- **Recipient**: is to whom personal data are released. This includes processors.
- **Third party**: is someone different from the data subject, controller or processor who is authorized to process personal data.
- **Representative**: a natural or legal person designated by a controller or processor, not established within the EU.
- **Data Protection Officer (DPO)**: is a person that must be designated under some circumstances (Article 37). Within its duties, DPO advise the controller or the processor, and monitor compliance with GDPR. (Article 39).

B. Research background

The assessment of privacy policies has been a big concern in recent years in the health domain, particularly in mHealth due to its rapid growth.

Contissa et al. [19] present a GDPR-based methodology to assess privacy policies. This methodology checks if a privacy policy includes all the information required by the articles 13 and 14 of the GDPR, if it is fair, and if it can be easily understood. The paper assesses 14 online platforms using this methodology and tries to automate the assessment. However, they do not develop a scale.

GDPR's requirements and recommendations from the Information Commissioner's Office of United Kingdom are used by [20] to design a privacy policy based on icons and highlighted text (called "GDPR label"). Their purpose is to compare a text-only GDPR with a GDPR label version. The labels capture all the information that is required to be included in privacy policies. This survey suggests that GDPR label version is preferred to text-only version.

Machine learning and natural language processing techniques are used in [21] to classify privacy policies. They use different GDPR articles to build a list of items to be assessed. A level of risk is associated to each item, depending on how a privacy aspect is addressed by the privacy policy. They have developed an application that receives a privacy policy as an input and then summarize this policy using a graphical user interface, so that users can easily identify potential risks in the privacy policy.

Renaud and Shepherd [22] make an exhaustive state-of-the-art research and a synthesis of GDPR requirements to provide a guide to write privacy policies. They focus on usability.

The articles above are referred to general privacy. However, privacy is especially important in the mHealth context. Some privacy papers focused on mHealth are discussed below.

A heuristic assessment approach is proposed in [23] to assess mHealth applications for self-tracking. They use different sources (such as GDPR or usability) to build a list of 26 heuristics in four categories (notice or awareness; choice or consent; access or participation; and social disclosure usability). Then they analyze 64 self-tracking applications to check if they comply with their heuristics. They develop a scoring method, but they are not exclusively based on GDPR as a source for the heuristics.

On the other hand, [24] assess privacy risks on 79 applications certified as safe by the UK National Health System. Unlike other assessments, they enumerate a series of topics for privacy policies, based on Information Commissioner's Office of United Kingdom and the Data Privacy Act of 1998 (repealed nowadays). Then they analyze if every topic has been addressed or not in the privacy policy of the assessed applications.

An analysis of the 600 most used mHealth applications as of May 2013 is presented in [25]. It shows that only 30% of the applications had a privacy policy on that date. They also analyze the average length of the privacy policies and assess the transparency of the privacy policies based in items considered most important by users.

A comparison of diabetes and mental health Indian applications is presented in [26]. They use readability tests and other readability metrics (such as word count and words per sentence) to conclude there is no significative difference between the two types of applications.

III. Methodology

A. Privacy scale design

Analyzing privacy in mobile applications is not a simple task. There are many factors that affect privacy. Some of them can be analyzed by auditing the app itself, while others require auditing the application's provider (for example, to check if its internal procedures comply with GDPR).

In the one hand, auditing the application includes analyzing security measures to verify if the application contains any known vulnerability or checking if the requested data are necessary for the purpose of the application. On the other hand, auditing the application's provider is related with the concept of accountability described above. Thus, the controller must implement a security policy in order to protect personal data, must deploy a privacy policy, must keep records of processing activities and, when necessary, must carry out a data protection impact assessment before processing data.

In this paper we focus on the document that describes the privacy policy since it is the first point of contact between the user (known as 'data subject' in the GDPR) and the application provider. Privacy policy is one of the pillars of privacy. This way, GDPR puts emphasis on the privacy policy and the information that must be provided to the data subject, when processing personal data. Our objective in this paper is to analyze any privacy policy in a systematic way so that we can obtain a score to assess the quality of privacy.

Article 13 of GDPR establishes the kind of information that must be provided to the data subject if the app collects data from him/her. Moreover, personal data must be processed in a transparent manner, according to article 5. Therefore, it is essential to verify that information given is coherent with the obligation of transparency. We also consider the recommendations of the Spanish supervisory authority on privacy policies [27, 28]. This way, we define a scale that builds a privacy score based on some of the features of the application privacy policy. The considered items and the score for all of them are the following:

- **Identity of the data controller**: 0 points if the identity is omitted, 0.5 points if only partial information is given and 1 point if full data is provided (including name of the data controller, postal address and electronic address).
- **Identity of the representative** when the controller is outside the EU. 0 points if no representative is identified and 1 point if it is. This item is not applicable (N/A) if the data controller is inside the EU.
- **Contact details of the DPO**: 0 points if no information is provided and 1 point if contact information is provided. In large scale mHealth applications, we must be aware of article 37 of GDPR, as it mandates that a DPO must be designated in this case.
- **Purposes of the processing**: 0 points if no purpose is provided, 0.5 points if the information provided is too generic and 1 point if specific information is given.
- **Legal basis for the processing**: Possible legal bases are enumerated in article 6 of GDPR. 0 pts if no legal bases are provided, 1 point if they are.
- **Legitimate interests:** if the processing is based on legitimate interest from the controller. 0 points if no information is provided, 1 point if it is. This item does not apply (N/A) if the legal bases for the processing are different from legitimate interest.
- **The recipients or categories of recipients of the personal data**: 0 points if the recipients are not provided, 1 point if they are. We consider that this information must be given even if there are no recipients of the collected data.
- **Transfers of personal data to a third country (outside the European Union):** 0 points if no information is provided, 0.5 points if the information provided is too generic, and 1 point if specific information is given (for example, if recipient holds a recognized certification such as Privacy Shield [29]). We consider that this information must be given even if there are no transfers.
- **Data storage period**: 0 points if no information is provided, 0.5 points if the information provided is too generic and 1 point if the period is given or, at least, the criteria to determine that period.
- **Existence of data subject's rights**: 0 points if no rights are pointed out, 0.5 points if the information provided is too generic and 1 point if specific rights and a method to exercise these rights are enumerated.
- **Existence of the right to withdraw consent at any time**: 0 points if no information is provided and 1 point if it is. This item does not apply (N/A) if data subject's consent is not a legal base for processing.
- **Right to lodge a complaint with a supervisory authority**: 0 points if no information is provided, 0.5 points if information provided is too generic and 1 point if specific information is given (such as the contact of the supervisory authority).
- **Obligation of providing data:** whether the provision of personal data is a contractual requirement, or a requirement necessary to enter into a contract. This item also considers whether the data subject is obliged to provide the personal data and the possible consequences of failing to provide such data. 0 points if no information is provided, 1 point if it is.
- **Existence of automated decision-making, including profiling**: 0 points if no information is provided, 0.5 point if information provided is too generic, 1 point if specific information about the logic used and the possible consequences to the data subject is provided. Also 1 point if there is no profiling and it is mentioned.

Table I shows a summary of all the defined items. We also include an item number for future references in this paper.

TABLE I. ITEMS IN THE PRIVACY ASSESSMENT

Item	Item No.	Score
Identity of data controller	1	0: no info; 0.5: partial; 1: full
Identity of the representative	2	0: no info; 1: Infor provided; N/A: not applicable
DPO details	3	0: no info ; 1: Info provided
Purposes for the processing	4	0: no info; 0.5: generic; 1: specific
Legal basis for the processing	5	0: no info; 1: Info provided
Legitimate interests from controller	6	0: no info; 1: info provided; N/A: not applicable
Recipients (or categories) of the personal data	7	0: no info; 1: info provided
International transfers of data	8	0: no info; 0.5: generic; 1: full details or no international transfers
Period for which data will be stored	9	0: no info; 0.5: generic; 1: specific
Existence of data subject's rights	10	0: no info; 0.5: generic; 1: full
Existence of right to withdraw consent	11	0: no info; 1: info provided; N/A: not applicable
Right to lodge a complain with a supervisory authority	12	0: no info; 0.5: generic; 1: specific
Obligation to provide personal data	13	0: no info; 1: info provided
Existence of automated decision-making or profiling	14	0: no info; 0.5: generic; 1: specific or no profilling/automated decision done

B. *Methods*

A systematic search was carried out on 30th January 2019, in the Spanish version of the two leading mobile app stores: Apple Store and Google Play. All relevant mHealth apps for BC were identified using the keywords "breast cancer".

Firstly, duplicates were removed. For those apps developed for both operating systems, iOS and Android, only Android version was selected. Titles and descriptions of the resulting mHealth apps were reviewed and assessed for eligibility against the selection criteria.

Inclusion criteria:

- App is intended for BC patients
- App is focused exclusively on BC
- App contains user information or allows user to share their opinions/data

Exclusion criteria:

- Description is not written in English
- Privacy policy is not written in English nor in Spanish if available
- App is not focused on BC
- App is focused on cancer in general, although BC is mentioned in the store description.
- App is not focused on BC self-management or support
- Apps intended for others than BC patients

IV. RESULTS

App stores searches resulted in 154 mHealth apps both in Apple Store (24.7%; n=38) and Google Play (75.3%; n=116). After removing duplicates, titles and descriptions of 148 mHealth apps were assessed for eligibility by two researchers. Discrepancies were resolved by consensus. Finally, 10 mHealth apps met the selection criteria. One of them was excluded due to not being freely available. The remaining 9 mHealth apps were downloaded to assess the privacy policy applying the proposed scale. Another one was excluded after installing it due to failure in the required register process. Table II shows the selected applications considering the inclusion/exclusion criteria. For convenience when analyzing the results, applications were tagged from app1 to app8.

TABLE II. SELECTED APPLICATIONS

App name	Developer	Operating System	Label
Becca – Support and Guidance	Breast Cancer Care	Android	App1
My Breast Cancer Coach	Genomic Health, Inc.	Android	App2
Breast Cancer Support	MyHealthTeams	Android	App3
OWise Breast Cancer	Px HealthCare B.V.	Android	App4
Boobytrapp – The Breast Cancer App	Boobytrapp	Android	App5
Breast Cancer Manager	@Point of Care	iOS	App6
Breast Cancer Ally	The University of Michigan	iOS	App7
Breast Cancer Survivor	Portable Medical Technology	iOS	App8

To obtain the privacy policies for the applications, we first downloaded them using the link provided in the application page in the corresponding application store (Google Play or App Store from Apple). If no link was provided, we looked for a privacy link in the developer's web. Then, we installed the applications in a smartphone, used it, and checked if the privacy policy was the same as the one shown in the developer's website.

Most of applications (5 out of 8) did not present any problem with their privacy policies. However, app1 privacy policy in the application store was different from the one available when using the application. Thus, the latter was analyzed. In addition, we were not able to use app7 because it asked for a PIN from a doctor or hospital. In this case, we have used the policy available in the developer's web page. Finally, app8 does not have an available privacy policy, neither in the developer's web (privacy policy is applied to all the services provided by the developer) nor in the app itself. Thus, we decided not to consider this application.

Some bad intention was observed in some of the applications. App3 privacy policy is ambiguous about the personal data that they process. Their developers claim that they do not collect user-specific identifying information, just to say afterwards to whom they do share personal information. Moreover, app5 developers claim that they do not hold any personal identifiable data, but they allow storing photos and audio, which might be used to identify people. Besides, they declare that they comply with GDPR, what is illogical with not processing personal data.

Table III shows the scores obtained after assessing the privacy policies of the 7 apps. We defined a percentual score. A score of 100 means a total accomplishment of GDPR. If an item is not applicable, it is not considered in the final score.

TABLE III. PRIVACY SCORES

App name	Label	Operating System	Score
Becca – Support and Guidance	App1	Android	57.7
My Breast Cancer Coach	App2	Android	25.0
Breast Cancer Support	App3	Android	78.6
OWise Breast Cancer	App4	Android	31.8
Boobytrapp – The Breast Cancer App	App5	Android	29.2
Breast Cancer Manager	App6	iOS	71.4
Breast Cancer Ally	App7	iOS	34.6

The first issue we notice is the low level of compliance with the GDPR in general. Only 3 out of 7 privacy policies score at 50% or higher. The highest score reaches 78.4% and the lowest one only scores 25.0%.

All privacy policies give full or partial information about the identity of the data controller and do specify the categories of recipients of personal data (Items 1 and 7). We consider that this is positive aspect. In addition, all applications except one explain the purposes for the processing (Item 4). This contrasts with the fact that none of the 5 applications whose data controller is outside the EU identifies a representative (Item 2). Not informing about the identity of the representative is considered a serious infringement under the Spanish data-protection law [30].

Although the Data Protection Officer (DPO) is compulsory when processing special categories of data at large scale (such as data concerning health), only 2 applications have designated a DPO (Item 3).

Privacy policies do not inform properly about user's rights, such as the rights to access, correct or delete information (Item10). Only 3 of the applications give enough information about user's rights, 1 of them gives only partial information and 3 of the policies do not even mention these rights. Furthermore, only 3 apps mention the data subject's right to lodge a complaint with a supervisory authority (Item 12). Moreover, they do not detail some aspects, such as how to find contact information of the supervisory authority.

Privacy policies also suffer from lack of information regarding the existence or not of profiling techniques. Only 3 policies inform users about the existence of profiling, but they do not give much information about the process, regardless GDPR statements (Item 14). Besides, 4 of the policies give some information about how long personal data will be stored (Item 9). 3 of the policies do not point out the legal basis for the processing (Item 5). Item 5 is important, since having a legal basis for the processing is the first item that should be accomplished, and not considering it is a very negative aspect.

Regarding the information about transfers to a third country, only 2 applications fully inform users about the transfers outside the EU (Item 8). 2 of them inform about the location of the data treatment but do not describe the measures prescribed by GDPR. Finally, 3 applications do not point out where the data are stored.

We did not find any relevant conclusions for Items 6 and 11.

Table IV summarizes the results that have been explained above.

TABLE IV. ACCOMPLISHMENT OF GDPR ITEMS SUMMARY

Item No.	Full information	Partial information	No information	Not applicable
1	5	2	0	0
2	0	0	5	2
3	2	0	5	0
4	5	1	1	0
5	4	0	3	0
6	2	0	1	4
7	7	0	0	0
8	2	2	3	0
9	2	2	3	0
10	3	1	3	0
11	3	0	1	3
12	0	3	4	0
13	1	0	6	0
14	0	3	4	0

V. CONCLUSIONS

Since privacy is one of the main concerns of breast cancer (BC) patients, it is important to analyze whether mobile applications comply with the recommendations of the authorities. In this paper, we have analyzed the privacy policy of 8 mobile applications for BC patients to check if they comply with the General Data Protection Regulation (GDPR). With this aim, we designed a scale to assess some of the items that must be complied by the apps.

Our scale builds a privacy score based on some of the features of the application privacy policy. We defined a percentual score, where a 100-point score means a total accomplishment of GDPR. The low level of compliance with the GDPR was quite surprising, as only 3 out of 7 privacy policies reached a 50-point score.

As positive aspects, all privacy policies give full or partial information about the data controller. Nearly all of them explain the purposes for the processing, and most of them specify how long they store the data.

As negative features, only 2 apps have designed a Data Protection Officer, only 3 of them inform the users about all their rights, just 3 of them report about the existance of profiling techniques, and another 3 do not point out where the data are stored. Legal bases are also often forgotten. Furthermore, when the apps are outside the EU, none of them identify a representative in the EU, while only 2 fully inform the users about the transfers outside the EU.

Thus, we conclude that there is still a long way to the whole compliance of GDPR. App developers must be concerned about this matter.

REFERENCES

[1] World Health Organization. "Global Status Report on Noncommunicable Diseases 2014", ISBN 9789241564854, 2014.

[2] R.L. Siegel, K. D. Miller, and A. Jemal, "Cancer statistics, 2016". CA Cancer J. Clin, vol. 66(1), 2016, pp. 7-30.

[3] A. K. Arrington, L. Goldstein, L. Kruper, C. Vito, J. Yim, and S.L. Chen. "Life expectancy after curative-intent treatment of breast cancer: Impact on long-term follow-up care". Am. Surg, vol. 80(6), 2014, pp- 604-609.

[4] S.P. Leong, Z.-Z. Shen, T.-J. Liu, G. Agarwal, T. Tajima, N.-S. Paik, K. Sandelin, A. Derossis, H. Cody, and W.D. Foulkes. "Is breast cancer the same disease in Asian and Western countries?". World J. Surg, vol 34(10), 2010, pp. 2308-2324.

[5] R. De Angelis, M. Sant, M. P. Coleman, et al., and EUROCARE-5 Working Group, "Cancer survival in Europe 1999–2007 by country and age: results of EUROCARE-5—a population-based study" Lancet Oncol., vol. 15 (1), Jan. 2014, pp. 23-34.

[6] J. Cho, S.-Y. Jung, J. E. Lee, E.-J. Shim, et al. "A Review of Breast Cancer Survivorship Issues from Survivors' Perspectives" J. Breast Cancer, vol. 17 (3), Sep. 2014, p.189.

[7] M.E. Hewitt, A. Bamundo, R. Day, and C. Harvey. "Perspectives on post-treat- ment cancer care: qualitative research with survivors, nurses, and physicians". J Clin Oncol, vol. 25, 2007, pp. 2270-3.

[8] B. Caulfield, and S. Donnelly. "What is Connected Health and why will it change your practice", *QJM*, vol. 106(8), 2013, pp. 703-7.

[9] R. Whittaker. "Issues in mHealth: findings from key informant interviews", J. Med. Internet Res, vol. 14 (5), 2012, e129, available at: http://dx.doi.org/10.2196/jmir.1989. Last consulted: February 2019

[10] W.T. Riley, D.E. Rivera, A.A. Atienza, W. Nilsen, S.M. Allison, and R. Mermelstein. "Health behavior models in the age of mobile interventions: are our theories up to the task?". Transl Behav Med, vol. 1, March 2011, pp. 53-71 [FREE Full text] [doi: 10.1007/s13142-011-0021-7] [Medline: 21796270]

[11] G. Giunti, D.H. Giunta, E. Guisado-Fernandez, J.L. Bender, and L. Fernandez-Luque. "A biopsy of Breast Cancer mobile applications: state of the practice review". International Journal of Medical Informatics, vol. 110, 2018, pp. 1–9, available at: https://doi.org/10.1016/J.IJMEDINF.2017.10.022. Last consulted: February 2019

[12] S. M. Phillips, D. E. Conroy, S. K. Keadle, C. A. Pellegrini, G. R. Lloyd, F. J. Penedo, and B. Spring. "Breast cancer survivors' preferences for technology-supported exercise interventions". Support. care cancer Off. J. Multinatl. Assoc. Support. Care Cancer, May 2017.

[13] N. H. Nguyen, N. T. Hadgraft, M. M. Moore, D. E. Rosenberg, C. Lynch, M. M. Reeves, and B. M. Lynch. "A qualitative evaluation of breast cancer survivors' acceptance of and preferences for consumer wearable technology activity trackers", Support. Care Cancer, vol. 25 (11), 2017, pp. 3375–3384.

[14] N. Ribeiro, L. Moreira, A. Barros, A.M. Almeida, and F. Santos-Silva. "Guidelines for a cancer prevention smartphone: A mixed-methods study", International Journal of medical Informatics, vol. 94 (1), October 2016, pp. 134-142.

[15] M. C. Robertson, E. Tsai, E. J. Lyons, S. Srinivasan, M. C. Swartz, M. L. Baum, and K. M. Basen-Engquist, "Mobile Health Physical Activity Intervention Preferences in Cancer Survivors: A Qualitative Study," *JMIR mHealth uHealth*, vol. 5, no. 1, p. e3, 2017.

[16] G. Giunti, J. Kool, O. Rivera Romero, and E. Dorronzoro Zubiete. "Exploring the Specific Needs of Persons with Multiple Sclerosis for mHealth Solutions for Physical Activity: Mixed-Methods Study", JMIR mHealth uHealth, vol. 6 (2), Feb. 2018, e37.

[17] S. R. Stoyanov, L. Hides, D. J. Kavanagh, O. Zelenko, D. Tjondronegoro, and M. Mani. "Mobile app rating scale: a new tool for assessing the quality of health mobile apps.", JMIR mHealth uHealth, vol. 3 (1), Mar. 2015, e27.

[18] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", EUR-Lex, available at: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04. Last consulted: February 2019.

[19] G. Contissa, K. Docter, F. Lagioia, M. Lippi, H.-W. Micklitz, P. Palka, G. Sartor, and P. Torroni. "Automated processing of privacy policies under the EU general data protection regulation". 31st International Conference on Legal Knowledge and Information Systems, JURIX 2018, Het KasteelGroningen, Netherlands, Volume 313, pp. 51-60, doi: 10.3233/978-1-61499-935-5-51.

[20] G. Fox, C. Tonge, T. Lynn, and J. Mooney. "Communicating compliance: Developing a GDPR privacy label". 24th Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018, Hyatt Regency New Orleans, United States.

[21] W.B. Tesfay, P. Hofmann, T. Nakamura, S. Kiyomoto, and J. Serna, "Privacyguide: Towards an implementation of the EU GDPR on internet privacy policy evaluation", IWSPA 2018 - Proceedings of the 4th ACM International Workshop on Security and Privacy Analytics, 2018, pp. 15-21, Tempe, United States, doi: 10.1145/3180445.3180447

[22] K. Renaud, and L.A. Shepherd. "How to make privacy policies both GDPR-compliant and usable", 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, 2018, Article number 85514422018, Glasgow; United Kingdom, doi: 10.1109/CyberSA.2018.8551442.

[23] L. Hutton, BA. Price, R. Kelly, C. McCormick, AK. Bandara, T. Hatzakis, M. Meadows, and B. Nuseibeh, "Assessing the Privacy of mHealth Apps for Self-Tracking: Heuristic Evaluation Approach", JMIR Mhealth Uhealth 2018;6(10):e185, doi: 10.2196/mhealth.9217.

[24] K. Huckvale, J.T. Prieto, M. Tilney, P-J. Benghozi, and J. Car. "Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment", BMC Medicine201513:214, doi: 10.1186/s12916-015-0444-y.

[25] A. Sunyaev, T. Dehling, P.L. Taylor, KD. Mandl, "Availability and quality of mobile health app privacy policies", J Am Med Inform Assoc. 2015 Apr;22(e1):e28-33, doi: 10.1136/amiajnl-2013-002605.

[26] A. Powell, P. Singh, and J. Torous, "The Complexity of Mental Health App Privacy Policies: A Potential Barrier to Privacy", JMIR Mhealth Uhealth 2018;6(7):e158, doi: 10.2196/mhealth.9871.

[27] Spanish data protection agency, "Informe sobre políticas de privacidad en Internet. Adaptación al RGPD", available at: https://www.aepd.es/media/estudios/informe-politicas-de-privacidad-adaptacion-RGPD.pdf. Last updated: September 2018. Last consulted: February 2019.

[28] Spanish data protection agency, "Decálogo para la adaptación al RGPD de las políticas de privacidad en Internet", available at: https://www.aepd.es/media/estudios/decalogo-politicas-de-privacidad-adaptacion-RGPD.pdf. Last updated: September 2018. Last consulted: February 2019.

[29] European Comission, "Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176)", available at: https://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj. Last updated: July 2016. Last consulted: February 2019.

[30] Spanish Official State Gazette, "Ley orgánica de protección de datos y garantía de derechos digitales", available at: https://www.boe.es/eli/es/lo/2018/12/05/3. Last updated: September 2018. Last consulted: February 2019.