Assessment of the quality of user awareness of GDPR in healthcare IOT

Kadir Ider
Dept. of Industrial Management
Technical University of Varna
Varna, Bulgaria
ORCID-ID: 0000-0001-8025-5772

2021 International Conference on Biomedical Innovations and Applications (BIA) | 978-1-6654-4581-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/BIA52594.2022.9831287

***Abstract*— This analysis of study results examines the impact of the GDPR on connected medical technologies. Building on these findings, elements are identified that lead to lawful and responsible processing of personal data. Key observations reveal that effective privacy compliance suffers from ever shortening innovation cycles, frequent introductions of hardware- and software and the lack of privacy by design integration in the end-to-end data processing lifecycle. Further, the GDPR awareness of users has a mutual effect on organizational accountability. A symbiosis of psychological, legal and technological parameters provides the framework for GDPR compliance.**

Keywords—GDPR, privacy by design and default, IOT device compliance

I. INTRODUCTION

Medical Internet of Things (MIOT) [1] finds its place in our private lives gradually, through the integration of features in hardware and software in mobile phones or smartwatches. They constantly measure our health and provide basic diagnosis, which aims at positively contributing to our overall health. The same data may become accessible to medical professionals in case of regular health check-ups or emergencies. The downside is the increasing digital transparency and threatening of individuals' privacy, as they are consistently producing health data, while being exposed to cyber security risks. Since health data is considered as sensitive data according to Art. 9 General Data Protection Regulation (GDPR), a variety of additional measures must be put in place to ensure legitimate and effective data processing [2].

The European Data Protection Regulation enforces strict rules, irrespective whether analogue or digital processing activities take place. Therefore, it is key to create a trustworthy, fair and transparent environment for processing data generated by or attributable to individuals and enforcing accountable handling of data by the data controller. It is becoming an increasing challenge to ensure privacy compliance with the advancement of connected devices, improving computing power and decreasing storage costs.

The Internet of Things (IOT) healthcare market can be segmented into four main categories [3], incl. (1) patients and individuals, (2) diagnostics and research, (3) hospital and healthcare and (4) government authorities. While all segments interact in the processing of personal information, the focus will be placed on patients and individuals as the source of the data production and demonstrated by using the case of wearable healthcare devices, such as smartwatches.

II. EVOLUTION AND TRENDS OF THE IOT MEDICAL MARKET

A study projects that global healthcare-related IoT revenues will increase almost sixfold between 2016 and 2025 [3]. The adoption of wearables, in particular smartwatches and health tracker devices shows 38% of Millennials and 33% of Generation Z respectively own one device [4]. Although this study is conducted on UK residents, an independent global study shows a similar distribution [5], whereas 162 respondents, i.e., 38% of all responses, claim to have a smartwatch:

TABLE I. SMARTWATCH USERS CLUSTER

Proportional Smartwatch Distribution[a]		
Number of Smartwatches	***Generation Z***	***Millennials***
0	58,80%	64,40%
1	41,20%	35,40%
2	0,00%	0,20%

[a] See appendix for further details

III. GDPR CHALLENGES OF MEDICAL IOT DEVICES

A. Analysis Of A Data Processing Lifecycle

The revenue is not limited to the purchase of the devices but for services that involve the processing and insight generation of user centric health information in the post purchase phase [3]. The privacy impact is reflected in the potential data use cases for example, wearable edge devices with integrated sensors powered by algorithms have achieved a 98.1% accuracy in the identification of true positive Covid-19 cases [6]. In the experiment, conducted by Hassantabar, et al., with 87 individuals, data from physiological sensors, such as an integrated oximeter collected information on heart rate, skin temperature, oxygen saturation and blood pressure. An isolated analysis of this data poses low privacy risks, as the individual cannot easily be identified, singled out or inferred.

Consequently, if no personal identification is possible, the GDPR is not applicable according to Art. 4 and 11 [2]. However, such data is associated with individuals by nature of the underlying processing activity, which aims at providing health information to the respective person. In such circumstances, the linkability of different datasets facilitates an indirect identification of users. It is therefore inevitable to ensure data privacy through appropriate technical and organizational measures, which must be embedded into the design of the software that (1) collects, (2) transfers and stores and (3) processes the data for various purposes. These measures decrease potential opportunities for cyber-attacks and data misuse.

Effective privacy is therefore bilateral, i.e., it requires privacy by design and effective communication, to achieve GDPR compliance within the organization and towards users.

B. *Privacy Assessment And Impact On Individuals*

The challenges of meeting GDPR compliance in the deployment of IOT devices for end users is the provisioning of information appropriate to the particular circumstances [7]. According to the Article 29 Working Party, users must have the chance to be noticed, resp. access the privacy policy even in cases where the data collecting device does not provide a readable screen. This needs to happen just-in-time, i.e., just before the data collection for a designated purpose takes place.

An appropriate alternative is to include the privacy policy in the packaging, attaching it to the device but also adding a URL or QR code for easier accessibility. The combination of various methods increase the channels and thus accessibility to privacy modalities. Often, IOT devices lack large enough screens for long, text based communication. Hence, most of these devices are accompanied by mobile applications, which further provide a platform for communicating privacy terms. One solution to privacy communication on the IOT device is to abandon text as means of communication altogether and instead adopt picture based Privacy Icons as research shows [10]. Such icons can represent types and sources of data, means and location of processing as well as information about data being passed on to third parties. Subsequently whenever the information needs to be communicated to the data subject, a Privacy Icon can be displayed on the device's screen. Alternatively, additional privacy information corresponding to the icons may be made accessible to the individual via mobile interface.

Moving away from user facing privacy enhancing technology (PET), engineers also need to implement sufficient measures for data processing. Since health data is considered to be especially sensitive, these internal measures are equally important as the aforementioned ones. One example could be the limitation to processing personal data locally on the IOT device instead of transmitting it only for the data being processed elsewhere. This technology enhances privacy by preventing data falling into the wrong hands after leaving the device.

Such features are considered as privacy by design, as they "bake in" privacy into the entire product service chain and ultimately, ensure compliance in the end-to-end data lifecycle.

TABLE II. CROSSTAB OF USER RIGHTS AND DEVICE FREQUENCY

Distribution Of User Right Importance Proportional To Device Frequency			
Right to be informed about an upcoming data processing and details of the activity[b]	***Number Of Smartwatches Owned***		
	0	***1***	***2***
not important at all	4,10%	4,30%	0,00%
somewhat important	0,00%	0,60%	0,00%
important	38,10%	35,20%	0,00%
very important	57,80%	59,90%	100,00%

[b.] ranking of importance in the original survey is numerical, ranging from 0 to 3 (lowest to highest)

The table above shows that 95% (162 individuals) of all respondents owning one smartwatch state that it is a (very) important requirement to be informed about data collection activities.

While the table above displays the subjective importance of user rights, i.e., irrespective of any detailed knowledge on GDPR, a subsequent assessment reveals in depth perspectives of individuals privacy knowledge but also past engagement with privacy modalities. In particular, the number of smartwatch users who are (or are not) aware of GDPR data subject rights, as well as the proportion of the same respondents who have already exercised user rights.

Why is the assessment of the question "Have you already exercised your right to be informed" so important? First of all, whenever users engage with organizations where personal data is being collected, there is an obligation of organizations to provide consumer privacy policies and thus, informing individuals about the data processing modalities of the organization is a legal necessity. This constitutes that (1) organizations meet their obligations, irrespective of the quality of the policy content and (2) users exercise their right by opening and reading the policy. Users that are aware of the data subject right to be informed, will consequently be reflected in the true positive quadrants, see table four.

In the specific case of smartwatch users, the significance of data is assessed through a comparison of the sum of true positives and true negatives in proportion to the false positives. The false positives represent the number of users that expressed that they were not aware of their rights but at the same time claimed to have exercised their right to be informed. The larger the number of respondents that are "not aware of their rights but exercised them" the more likely it is an indicator that users (a) did not read or understand the questions correctly or (b) did not understand the respective subject rights. The smaller the number of the false positives in proportion to the sum of the true positives and true negatives, the more likely it is that the data reinforces the user responses. A slightly altered confusion matrix below summarizes this paragraph. The alteration is due to the fact that there is no actual and prediction class, but instead two actual classes. Therefore, there are two true positives as the third quadrant equivalently represents a true positive answer. To facilitate better understanding, Table 3 only provides the typology in the crosstab and Table 4corresponding proportional values.

TABLE III. TYPOLOGY CROSSTAB MATRIX

		Aware of user right[c]	
		Yes	***No***
Exercised User Right	Yes	1) True positive	2) False Positive
	No	3) True positive	4) True Negative

[c.] The labels used within the matrix shall not be conflated with the confusion matrix

TABLE IV. CROSSTAB MATRIX WITH PROPORTIONAL OBSERVATIONS

		Aware of user right	
		Yes	***No***
Exercised User Right	Yes	1) 51,00%	2) 9,00%
	No	3) 37,00%	4) 3,00%

The results show that 91% of individuals, i.e., sum of the true positives and true negatives, fulfil the above conditions, leaving just 9% of the respondents with inconsistent statements, reflected by the false positives (index number 2, in table 3). Thus, the data shows more than 90% of confidence in the data accuracy, leaving 10% of uncertainty.

978-1-6654-4581-8/22/$31.00 ©2022 IEEE

The preceding paragraph has one specific limitation. It evaluates the initial data collection process but does not take into account, if existing devices are used to collect new types of data. In the scope of medical IOT devices, this could mean that existing hardware is leveraged through updated software, which allows the collection of additional health data. In this scenario, organizations must ensure flawless GDPR compliance as well. Due to scope limitations, this will not be discussed further in the scope of this analysis.

IV. Trustworthiness Of IOT Devices

The following hypothesis is proposed, i.e., the trustworthiness of IOT devices with regards to the processing of personal data is directly related to the trust placed in organizations, whose brands are associated with such products.

From a privacy point of view, trustworthiness of IOT devices is strongly associated with the level of control over personal data [8]. Whilst both, the level of trust and control may possess uncorrelated features as well, the common elements are of higher significance due to their leverage power.

Increasing the trust towards IOT devices and control over the data processed through such, would therefore need to be assessed from three angles, ranked by importance

1) *psychological,*
2) *legal and*
3) *technological perspective.*

The psychological perspective may be the most significant as cultural and emotional values shape the perception of the level of control users can exercise on extraneous conditions and variables [9].

The evaluation of the psychological control perception across various dimensions strongly correlates with the provisioning of a simple user-friendly UI and UX. An essential discovery is the reduction of the time cost for reading policies and search of relevant privacy information. There is an extreme dichotomy between the actual time spent for reading policies, and thus, for spending time on privacy modalities versus the time needed to fully read such policy. Latter does not measure or imply the level of understanding but merely the time spent reading. Therefore, an initial step in the improvement of control and trustworthiness is the decrease of the burden for information search and the associated time cost [11] for accessing and processing such information via the IOT devices.

The underlying data shows that the user experience, i.e., perception of privacy modalities, its presentation, content, length, interface design and navigation essentially influence the time cost. Consequently, implementing the identified features will meet user behavior and improve engagement. The existence of a gap between self-reported and observed behaviors that have been analyzed in an external study [12] and validated in the scope of a survey conducted for this research paper.

The assessment is the backbone for user confidence in the exercise of their privacy rights under the GDPR, i.e., the exercise of user rights that must be proactively carried out by the organizations (controller and processor), the exercise of user rights under Art. 12, 13, and 14 GDPR. In addition, the interface must provide a service that enables individuals to exercise their rights under Art. 15,16. Users' assessment of the importance of user rights and their confidence in exercising those rights differ. The legal perspective provides the framework for lawful compliance, underlines and enhances the psychological elements, as stated in the table below:

TABLE V. Legal Control Over Data

User Control Elements Derived From GDPR Requirements	
Article	***Specification***
12	Transparent information, communication and modalities for the exercise of the rights of the data subject
13	Information to be provided where personal data are collected from the data subject
14	Information to be provided where personal data have not been obtained from the data subject
15	Data subjects right of access personal data
16	Data subjects right for rectification of personal data
17	Data subjects right for erasure (‘right to be forgotten’)
18	Data subjects right to restriction of processing
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing

Lastly, the technological element provides concrete technical and organizational measures to operationalize the legal requirements, which in turn facilitates the basis for enhancing to some extent the psychological view and thus closes the circle. This assessment is based on the reliability of data processing technology, while the underlying system is user-related, there is a growing need for plain language usage, easy access to information, and transparency of data processing technology. As with the requirements for a better understanding of privacy policies, the reliability of data processing technology begins with providing users with documentation of such technology.

While the psychological perspective represents the sole element that affect every single users inherent control perception, the legal and technological perspective represent the external factors that effectuate user awareness, improve individual judgment capabilities associated with effective exercise of rights.

Nevertheless, the symbiosis of all will impact the level of control and thus, trustworthiness of organizations with respect to the processing of personal data. This constitutes a GDPR awareness building framework.

V. Conclusion

At first sight of the 162 individuals that own a smartwatch, the number of individuals (95%) that state, it is a (very) important requirement to be informed about data collection activities is almost congruent with the sum of the true positives and true negatives (91%). However, merely 51% are aware and have exercised their right of information. This may suggest an ineffective communication of privacy modalities to individuals.

Applying the findings to IOT devices translates to a low operationalization and thus ineffective compliance with the GDPR. Particularly medical IOT devices collect sensitive

978-1-6654-4581-8/22/$31.00 ©2022 IEEE

information on individuals, where a misconduct, i.e., misuse of personal information may cause severe implications on individuals and could lead to high monetary penalties for corporations. It is therefore strongly suggested to improve the privacy communication by designing features embedded into the data lifecycle, as presented in the preceding chapters.

Ultimately, the analysis identifies multiple parameters that mutually affect the GDPR awareness of users, ranging from the implementation of technical and legal privacy design features over the consideration of psychology in the user experience design.

REFERENCES

[1] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, Security and Privacy in the Medical Internet of Things: A Review, Security and Communication Networks, 2018 e5978636.

[2] General Data Protection Regulation (2016), 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), OJ 2016 L 119/1.

[3] The Insight Partners, "IoT in Healthcare Market to 2025 - Global Analysis and Forecasts by Solution", The Insight Partners, 2016. Available at: https://www.theinsightpartners.com/reports/iot-healthcare-market

[4] Attest, "Generational Trends Report 2019", 2019. Available at: https://www.askattest.com/resources/generational-trends-report-2019

[5] K. Ider, "Survey - Complexity reduction and operationalization of the GDPR: Conceptualization of a user-oriented online privacy control system and evaluation of its effects towards corporate trust" unpublished.

[6] S. Hassantabar, N. Stefano, V. Ghanakota, A. Ferrari, G.N. Nicola, R. Bruno, I.R. Marino, K. Hamidouche, N.K. Jha, "CovidDeep: SARS-CoV-2/COVID-19 Test Based on Wearable Medical Sensors and Efficient Neural Networks", ArXiv:2007.10497 [Cs], 2020.

[7] Article 29 Working Party (2017) "Guidelines on transparency under Regulation 2016/679". Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013. Available at: https://ec.europa.eu/newsroom/article29/items/622227.

[8] J. B. Lyons, C. K. Stokes, K. J. Eschleman, G. M. Alarcon & A.J. Barelka (2011) "Trustworthiness and IT Suspicion: An Evaluation of the Nomological Network". Human Factors [Online], 53 (3) June, pp. 219–229. Available from: <https://doi.org/10.1177/0018720811406726> [Accessed 23 December 2020].

[9] G. R. VandenBos, ed. (2015) APA Dictionary of Psychology (2nd Ed.). Washington: American Psychological Association.

[10] L. F. Cranor (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. J. on Telecomm. & High Tech. L., 10, 273.

[11] A. M. Mcdonald, & L. F. Cranor, (2008) The Cost of Reading Privacy Policies. I/S: A Journal Of Law And Policy, 4:3, pp. 544–568.

[12] S. Kokolakis, (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. Computers & Security 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

APPENDIX

Referring to Table 1: Calculation of Generation Z and Millenials is based on the original data collected. Generation Z covered by the age group of 20 - 25 year olds and Millennials respectively by 26 - 30, 31 - 35 and 36 - 40.

The table below shows the absolute values, n = 431.

TABLE VI. DETAILS ON THE SGE GROUP CALCULATION

	Age Group						
	20-25	***26-30***	***31-35***	***36-40***	***40-45***	***46-50***	***51-55***
#[d]	***Absolute Values***						
0	20	101	76	43	22	1	5
1	14	52	63	16	12	1	4
2	0	1	0	0	0	0	0
#[d]	***Proportional Distribution***						
0	58,8%	65,6%	54,7%	72,9%	64,7%	50,0%	55,6%
1	41,2%	33,8%	45,3%	27,1%	35,3%	50,0%	44,4%
2	0,0%	0,6%	0,0%	0,0%	0,0%	0,0%	0,0%

[d] Number of smartwatch devices owned

978-1-6654-4581-8/22/$31.00 ©2022 IEEE