User Privacy in Health Monitoring Wearables

Requirements stemming from current and proposed European Union legislation

Kiril Kalev, Jernej Mavrič, Sophie Pijnenburg, Anouk de Ruijter
Tilburg Institute of Law, Technology, and Society
Tilburg University
Tilburg, the Netherlands
e-mail: {k.z.kalev, j.mavric, s.k.j.pijnenburg, a.deruijter}@tilburguniversity.edu

***Abstract*—Health monitoring wearables are a new type of mobile devices that are worn on the user's body and are becoming a huge trend. These devices (and the respective software needed to run the services) can track data like heartbeat and blood oxygen level, which are rightfully considered as sensitive data. If these data fall into the wrong hands, this could have serious consequences. To what extent do the five selected wearables comply with current and proposed EU data protection legislation and (how) can the privacy policies be improved? The EU is currently negotiating a new data protection regulation that will replace the Data Protection Directive. Therefore, the focus will be on the new General Data Protection Regulation (GDPR). It turns out that most market players in the field of health monitoring wearables are not ready for the coming into force of the GDPR. This paper proposes a number of improvements to better prepare data controllers for the upcoming regulation and strengthen the privacy rights of consumers.**

Keywords: health monitoring wearables; user privacy; EU legislation; compliance with legislation; data protection.

I. INTRODUCTION

Wearable technology is getting more and more implemented in our daily lives. This innovation can alter the landscape of society and business as we know it [1]. For example, the use of wearable technology in employer-sponsored health programs can lead to a healthier and more productive workforce. However, there is also a downside, using health monitoring wearables can lead to privacy risks because of the privacy-sensitive nature of the data that the applications track. When third parties, such as future employers or insurance companies have access to this sensitive data, they can adapt their agreements and policies to the specific person, not always in the advantage of the wearable user.

A. Health monitoring wearables

Health monitoring wearables track activity-related data such as steps taken, distance and calories burnt and are expected to help people achieve a (more) healthy lifestyle. The Misfit Shine [2], TomTom Runner Cardio [3], Samsung Gear Fit [4], Medisana ViFit Connect [5] and the Withings Pulse Ox [6] are analysed. The devices have been selected by the Tilburg Institute for Law, Technology, and Society to represent the diversity in the available wearables. The devices have their own smartphone and/or desktop app and some even share data with other weight loss or fitness apps.

All apps track steps and distance travelled, calories burnt and sleeping time. The Withings Pulse Ox also measures the user's heart rate, blood oxygen level and tracks sleeping cycles. Samsung Gear Fit can also measure the user's heart rate and can show incoming notifications on its screen (see Figure 1).

	Steps	Distance	Calories	Speed	Elevation climbed	GPS tracker	Sleeping time	Sleeping cycles	Heart rate	Blood oxygen level	Messages & calls	Agenda
Misfit Shine	✓	✓	✓	X	X	X	✓	X	X	X	X	X
Samsung Gear Fit	✓	✓	✓	X	X	X	✓	X	✓	X	✓	✓
Withings Pulse	✓	✓	✓	X	✓	X	✓	✓	✓	✓	X	X
TomTom Runner Cardio	✓	✓	✓	✓	X	✓	X	X	X	X	X	X
Medisana ViFit Connect	✓	✓	✓	X	X	X	✓	X	X	X	X	X

Figure 1. Functionalities of selected wearables.

B. Legal perspective

From a legal perspective, the predominant legal basis for processing personal data collected by the analysed wearables, is consent. Users are expected to agree with terms and conditions that they may not have read, let alone have understood, ultimately resulting in a lack of the elements of a valid consent.

This paper discusses the obligations of controllers and processors of personal data and conducts an assessment for compliance with existing and proposed legislation in this

 ISBN: 978-1-61208-446-6

field, with an emphasis on the latter. The current EU legislation that applies to the processing of personal data, is the Data Protection Directive (DPD) [7] along with a few other legal acts, such as the E-Privacy Directive [8]. The EU is currently negotiating new data protection laws. It is foreseen to replace the DPD with a regulation, a legislative instrument directly binding upon all EU member states.

The General Data Protection Regulation (GDPR) [9] will likely come into force in 2018 [10]. One of the novelties that the GDPR brings is a set of six graphical forms, each representing a different requirement that data processors must use to comply with information obligations laid down in the GDPR. Each of them should be accompanied by either a checkmark on green background, representing compliance, or a cross on red background, standing for non-compliance.

The analysis includes both the devices as such and the corresponding privacy policies of the services listed in [2] until and including [6]. For the sake of conciseness, the service providers are referred to with their popular commercial names (e.g., Samsung instead of Samsung Electronics (UK) Limited). Citations used as examples have been taken from the above listed privacy policies.

C. Structure

Section 2 of the paper will describe important definitions, the obligations lying on the controllers and will also focus on the differences between the current and proposed regulation. Section 3 will compare the privacy policies of the wearables with the current and new regulation to assess if they are compliant and proposes a number of improvements. A table containing the graphical forms will be presented in the same section as an example of a correct implementation of the standardised information policies in practice. The paper will end with a conclusion in Section 4.

II. Concepts of Data Protection Legislation and the Changes the GDPR Will Bring

On January 25, 2012 a proposal for a data protection regulation was released. The GDPR will be directly applicable in all member states. The proposal aims at high data protection standards, which are better harmonised and fit for the internet age [11]. On March 12, 2014 the European Commission adopted the text with amendments (in first reading) [12]. The Parliament voted overwhelmingly in favour of the GDPR [13] and now it is up to the Council of Ministers to review the Regulation. This paragraph analyses the most important concepts of data protection regulation and the changes of the GDPR with regard to them.

A. Users of personal data

The users of personal data can either be controllers, processors, third parties or recipients. The distinction between these legal concepts is important because it determines who shall be responsible for compliance with the data protection rules, how data subjects can exercise their rights and what the applicable national law is. The definitions of users of personal data will likely remain the same under the GDPR.

A controller is "a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" (art. 4(5) GDPR). All of the researched service providers can be qualified as controllers. A processor is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (art. 4(6) GDPR). A third party is someone who is legally different from the data subject, controller or processor. Recipient is a broader term, the definition of which is someone to whom data are disclosed (art. 4(7) and 7(a) GDPR).

B. Personal data

Personal data is defined in the DPD as "any information relating to an identified or identifiable natural person". An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (art. 2(a) DPD). The GDPR broadens the definition of personal data by including more examples of identifiers.

C. Sensitive (health) data

Sensitive data, as a subcategory of personal data, includes health data. In contrary to the DPD, a definition of health data is given in the GDPR, namely "Data concerning health means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual" (art. 4(12) GDPR).

D. Data processing

Data processing is defined as "operation or set of operations which is performed upon personal data, whether or not by automated means", under art. 2(b) DPD. Slight changes have been made in the GDPR that do not affect the scope of the notion that this term covers.

E. Consent

Data processing is only allowed on the basis of a legal ground, listed in art. 7 DPD. Because wearables can collect sensitive data, the only remaining legal basis for legitimate data processing is consent (art. 8 DPD).

One of the major changes of the GDPR is the concept of consent. If no other legal ground is applicable, data subjects have to give their explicit consent for the processing and storing of personal data (art. 4(8) GDPR). Explicit consent is needed not only for sensitive personal data but for all personal data. The GDPR will require consent to be expressed by a statement or by a clear affirmative action. So, explicit consent will be given when data subjects sign a consent form that clearly outlines the purposes for which the

 ISBN: 978-1-61208-446-6

data is collected and processed. This could include ticking a box when visiting an internet website [14].

F. Quality principles

There are five main groups of principles relating to data quality. The qualities are set forth in art. 6(1)(a-e) DPD: lawfulness and fairness, purpose limitation, data minimisation, accuracy and storage minimisation. Art. 5 GDPR restates the five quality principles from the DPD with a few amendments. The principles of data minimisation, storage minimisation and purpose limitation are included in the standardised information policies as set out in art. 13a(1) GDPR. Each of these principles has its own corresponding pictogram which is part of the Annex to the Regulation named 'Presentation of the particulars referred to in article 13a'. The Annex explicitly states that compliance with these three requirements is "required by EU law".

III. Conducting an Assessment of Controllers' Privacy Policies Compliance With Statutory Obligations

The compliance assessment proved to be difficult to conduct because the privacy policies of the analysed wearables use vague expressions, lack details and do not address all the statutory requirements specifically. This mainly holds for storage minimisation and purpose limitation. Moreover, most of the policies do not address data retention and encryption.

This section points out the requirements the controllers do not comply with. Recommendations are made with regard to how these examples of non-compliance can be tackled. Emphasis is being put on the requirements as prescribed by the latest draft of the GDPR.

A. Data minimisation

All of the services have been estimated not to collect an excessive amount of personal data, thus being overall compliant with the data minimisation principle (see Figure 1), as laid down in art. 6(1)(c) DPD and art. 5(1)(c) GDPR. None of the privacy policies provide an exhaustive list of all the types of data collected and retained. However, collection of data such as the exact date of birth of the user required by Withings and Samsung might be considered excessive.

Firstly, because proving that the user is not a minor can be achieved through other means and secondly because just the year of birth would not unreasonably limit the functionalities of the services. Offering the option to use a non-identifying nickname instead of requiring the full name of the user, an approach used by Medisana, is another practical suggestion to promote the principle of data minimisation.

The GDPR pays extra attention to the principle in question by adding the requirement that "[data] shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data".

B. Purpose limitation

The service providers have given examples of the purposes for which data are collected, but the lists do not appear to be exhaustive so as to unambiguously comply with the purpose limitation requirement. This is laid down in art. 6(1)(b) DPD and art. 5(1)(b) GDPR and requires controllers to be specific and explicit with regard to data processing purposes.

Concerning the element of the same requirement that prescribes that data shall not be further processed in a way incompatible with purposes rather than the ones for which they were initially collected, all of the assessed service providers' privacy policies seem to be compliant (see Figure 2). However, this conclusion has been made solely on the basis that none of the service providers has hinted such a scenario. To avoid any confusion and to demonstrate responsibility, the service providers need to list all of the purposes for which the personal data are collected. Furthermore, they also need to state explicitly and clearly that they will not further process the collected personal data in a way incompatible with the initial purposes without the acquisition of a separate consent.

C. Access to data by third parties

None of the privacy policies explicitly mention that the collected personal data might be sold or rented out. Out of the five assessed policies only the Samsung privacy policy gives a clear example of disseminating personal data to commercial third parties. Even though the latter might be considered to be overlapping to a certain extent with the former, both are separate requisites under the GDPR. Samsung's privacy policy states that "[Samsung Electronics (UK) Limited] also may share your information with trusted business partners (…) [who] may provide you with promotional materials, advertisements and other materials".

While the service providers are not forbidden to share collected personal data with third parties in general, they still have to unambiguously indicate their conduct regarding the sharing of data. The approach undertaken by the controllers, with a single exception, namely not to explicitly address these requisites, leads to the lack of information for the users with regard to compliance with art. 13a(1)(d) and (e) GDPR (see Figure 2 for both requisites). A general recommendation to address this issue therefore is that all the controllers should clearly state if personal data are disseminated, whether or not by subcontractors, to commercial third parties. The same approach should also be applied to whether personal data are sold or rented out.

D. Storage minimisation and data retention

Art. 14(1)(c) of the GDPR introduces the requirement that either the period for which the personal data will be stored should be specified, or if this is not possible, at least the criteria used to determine this period should be

 ISBN: 978-1-61208-446-6

described. Only Samsung's privacy policy addresses this requirement by stating that information about the data subjects will be kept "only for so long as is necessary for the purpose for which it was collected". This wording is, however, too vague and not definite enough to fulfil the statutory requirement. Therefore, none of the controllers fully complies with this requirement (see Figure 2). Different types of data may be stored for different periods. A user-friendly approach to incorporate such a list in the privacy policy of a service would be to make use of multi-layered notices, as suggested by the Article 29 Working Party [15]. Such an approach can be a useful solution also for the listing of the types of data collected and the purposes for which they are going to be used.

After the purposes for which the user data were collected have been fulfilled these data should be erased. Otherwise, they should be anonymised or pseudonymised. These requirements are set out by art. 6(1)(e) DPD and art. 5(1)(e) GDPR. The process of anonymisation or pseudonymisation should, when possible, be already implemented in the stage of collecting data. This should only be the case when it will not lead to limitations of the functionality of the service.

E. Encryption

While encryption is voluntary under the GDPR, pursuant to art. 13a(1)(f) of this Regulation the service providers should still state whether personal data are retained in encrypted form. Only one of the assessed controllers complies with this requirement of the GDPR (see Figure 2). The requirement itself can be considered restrictive in naming a single amongst all possible technical measures to protect privacy. To fulfil this requirement the service providers should mention encryption explicitly. This does not mean that all other possible organisational and technical security measures should not be mentioned in the privacy policies, as the requirement for implementing such measures is prescribed by art. 17(1) DPD and art. 26(1) GDPR.

F. Information about the controller and processor

Pursuant to the requirements of art. 10(a) DPD and art. 14(1)(a) GDPR the controller must provide the data subjects with information about itself and its representatives, if any. In other words, the service providers, along with information about themselves, should also provide information about subcontractors or processors of user data. In case they do, the privacy policies should include the identity and the location of the processors and a description of the processing activities.

Samsung, for instance, in its privacy policy gives explicit examples of its affiliates and mentions that information may be passed on to sub-processors referred to as "service providers", whereas Medisana provides in its privacy policy the most information about the legal entity that serves as a controller. However, none of the assessed controllers gives enough information to fulfil all aspects of this requirement to a sufficient extent.

G. Data storage

The service providers should list the locations of all the servers where users' data are stored. The location should be specific enough, especially if the data are stored on a server located outside the European Economic Area (EEA). In the latter case, according to art. 26(1)(a) DPD and art. 44(1)(a) of the GDPR, the service providers should also point out which security and data protection standards does the server in question comply to. Out of the assessed service providers the best approach has been undertaken by TomTom by being clear and thorough enough in stating in its privacy policy that "TomTom and [their] partners and subcontractors have taken adequate security measures to protect [users'] information from unauthorized access. Some of these partners and subcontractors are located outside the EU. [They] have contractually bound them to provide a level of protection of [users'] data according to European data protection legislation and they take full responsibility and accountability for this". Still, this description lacks a list, exhaustive or not, of countries where data may be stored. Misfit, for instance, in its privacy policy provides a single example by stating that data may be transferred "globally, including to the United States".

H. Right of access to data

The users have the right to obtain from the service providers at any time, on request, confirmation as to whether or not personal data related to them are being processed, as well as detailed information on the processing activities. The description should be in clear and plain language pursuant to the requirement of art. 12(a) DPD and art. 15(1) GDPR. Furthermore, according to art. 12(b) DPD as well as art. 14(1)(d) and 17(1)(b) GDPR the users should also be provided with a procedure to rectify, erase or block their data on a number of grounds.

Most of the assessed service providers comply with these requirements. However, Samsung's privacy policy mentions that the service provider "may charge a reasonable fee for dealing with [access to data] request" and Withings requires in its privacy policy a "request by post to the address of Withings' registered office". Both approaches are undesirable for an Internet-based service. Misfit's privacy policy states that this service provider "currently [does] not have a way to let [the users] correct or update [their] personal information", thus explicitly declaring non-compliance with the rights in question.

IV. CONCLUSION

This paper examines a number of requirements under existing and new data protection legislation that might pose privacy and data protection risks for users of health wearables. This list is, however, not exhaustive, i.e., it does not address all obligations lying on data controllers.

To conclude, the selected controllers are not fully ready for the adoption of the GDPR and also do not fully comply with most of the current requirements under the DPD.

 ISBN: 978-1-61208-446-6

Compliance with the new requirements under the GDPR is advisable as it will provide a smooth transition for both controllers and users of the wearables by the time the new regulation comes into force. Non-compliance with the current legislation is, however, a serious issue that needs to be taken care of without delay.

To achieve this, every statutory requirement should be explicitly addressed in clear and plain language. The privacy policies are the only source of information for (prospective) users of the wearables. This is why compliance with a requirement in practice is not enough, stating it in writing is as important.

ACKNOWLEDGMENT

This paper is the result of a law clinic, a project by the Tilburg Institute for Law, Technology, and Society in cooperation with Louwers IP|Technology Advocaten, funded by the Law Alumni Fund. This project has been set up to enable students to gain insight into a specific area of law and see the practical implications of it. Special acknowledgments go to Marianne Korpershoek, Tom de Wit and Colette Cuijpers for the guidance during the project, and everyone at the Tilburg Institute for Law, Technology, and Society for their valuable feedback.

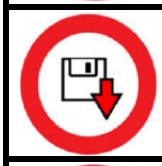
	EXPLANATION	MISFIT SHINE	TOMTOM RUNNER CARDIO	SAMSUNG GEAR FIT	WITHINGS PULSE OX	MEDISANA VIFIT CONNECT
	No personal data are collected beyond the minimum necessary for each specific purpose of the processing	✓	✓	✓	✓	✓
	No personal data are retained beyond the minimum necessary for each specific purpose of the processing	X	X	X	X	X
	No personal data are processed for purposes other than the purposes for which they were collected	✓	✓	✓	✓	✓
	No personal data are disseminated to commercial third parties	✓	✓	X	✓	✓
	No personal data are sold or rented out	✓	✓	✓	✓	✓
	No personal data are retained in unencrypted form	✓	X	X	X	X

Figure 2. Compliance chart.

 ISBN: 978-1-61208-446-6

REFERENCES

[1] PricewaterhouseCoopers B.V. Consumer intelligence series - The wearable future. [Online] Available from: https://www.pwc.se/sv_SE/se/media/assets/consumer-intelligence-series-the-wearable-future.pdf 2015.05.04

[2] Misfit Wearables. Privacy policy. Effective date: 2012.04.23 [Online] Available from: http://misfit.com/legal/privacy_policy 2015.02.11

[3] TomTom Mysports. Privacy. Effective date: 2013.06.01 [Online] Available from: https://mysports.tomtom.com/content/privacy 2015.02.11

[4] Samsung Electronics (UK) Limited. Local privacy policy. Effective date: 2014.03.10 [Online] Available from: http://www.samsung.com/uk/info/privacy.html 2015.02.11

[5] Vitadock+. Data privacy statement. Effective date: 2012.06.15 [Online] Available from: https://cloud.vitadock.com/privacy.html?lang=nl 2015.02.11

[6] Withings. Withings terms and conditions. [Online] Available from: http://www.withings.com/eu/terms-and-conditions#privacyrules 2015.01.15

[7] Directive 95/46/EC of 24 October 2014 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

[8] European Parliament. Fact sheets on the European Union. [Online] Available from: http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_5.12.8.html 2015.02.17

[9] Proposal for a Regulation of the European Parliament and of the Council COM(2012)0011 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2012] OJ C7-0025/12

[10] Allen & Overy. Radical changes to European data protection legislation. [Online] Available from: http://www.allenovery.com/publications/en-gb/data-protection/Pages/Timetable.aspx 2015.02.11

[11] P. de Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", Computer law & security review, vol. 28, April 2012, pp. 130-142.

[12] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2014] T7-0212/2014

[13] European Commission Press release database. Progress on EU data protection reform now irreversible following European Parliament vote. [Online] Available from: http://europa.eu/rapid/press-release_MEMO-14-186_nl.htm 2015.02.11

[14] W. Kotschy, "The proposal for a new General Data Protection Regulation—problems solved?", International Data Privacy Law, vol. 4, no. 4, November 2014, p. 278.

[15] Working Party 29 Opinion 11987/04/EN, WP 100 on on More Harmonised Information Provisions [2004], p. 6 [Online] Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf 2015.02.11

 ISBN: 978-1-61208-446-6