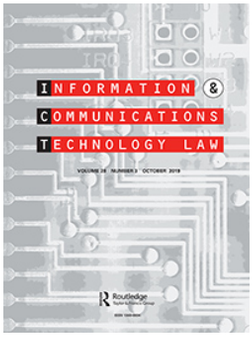
Privacy policies, cross-border health data and the GDPR

Mulder, T.; Tudorica, M.

Published in:
Information & Communications Technology Law Journal

DOI:
10.1080/13600834.2019.1644068

Publication date:
2019



Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Privacy policies, cross-border health data and the GDPR

T. Mulder & M. Tudorica

To cite this article: T. Mulder & M. Tudorica (2019) Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law, 28:3, 261-274, DOI: 10.1080/13600834.2019.1644068

To link to this article: https://doi.org/10.1080/13600834.2019.1644068

Published online: 19 Jul 2019.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
2019, VOL. 28, NO. 3, 261–274
https://doi.org/10.1080/13600834.2019.1644068

Routledge
Taylor & Francis Group

Privacy policies, cross-border health data and the GDPR

T. Mulder and M. Tudorica

Security Technology and ePrivacy Research Group, Faculty of Law, University of Groningen, Groningen, the Netherlands

ABSTRACT

Research going back to 2008 has shown that a vast majority of the people never read privacy policies (AM McDonald and LF Cranor, 'The Cost of Reading Privacy Policies' (2008) 4A JLPI 543). Since then, not a lot has changed (F Schaub and others, 'Designing Effective Privacy Notices and Controls' (2017) 99 IEEE 70). Most people formally consent to privacy policies without knowing what happens to their personal data. This odd situation is called the privacy paradox: while people highly value their fundamental right to privacy, they do not act accordingly, especially when it concerns new technologies (M Taddicken, 'The "Privacy Paradox" in the Social Web' (2013) 19 JCMC 248). Since more and more people use apps on their mobile phones and wearables to measure their health, it is important to do research in this area. Nowadays, privacy is a popular news item; this might be why more and more companies use privacy both in their business models and as a marketing tool. This raises the question whether people really give 'informed consent' to privacy policies, as they seem to rely on marketing statements rather than reading the actual privacy policies themselves.

KEYWORDS

Data protection; health data; cross-border; modern technologies; GDPR

Introduction

'Your privacy is important to us' is an often-used marketing statement companies use. Is this, however, reflected in their privacy policies? This paper examines the discrepancies between the marketing statements vis-à-vis the actual privacy policies of three health apps and wearables. These apps generate personal data and health data. Health data is considered sensitive data due to the great impact it could have on a person's life if these data were freely available. Moreover, due to the very nature of modern technologies, data are not necessarily bound by country or European Union (EU) borders. The new EU General Data Protection Regulation (GDPR)[1] legal framework provides rights for users of modern technologies (data subjects) and obligations for companies (controllers and processors) with regard to processing of personal data. However, does the complexity of the

CONTACT T. Mulder t.mulder@step-rug.nl

[1]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) [2016] OJ L 119/1.

legal framework reflect reality? In particular in view of the borderless aspect of these technologies?

We argue that there is a gap between European data protection legislation and practical reality as regards the use of modern technologies. This gap exists in particular when it comes to transparency, a vital element in the data protection legal framework. Transparency is important considering that it is intended to help users understand how their personal data are being processed and consequently help them make a choice between the various available health apps and wearables. Other gaps include the notion of informed consent and cross-border elements such as jurisdiction and the exercise of rights.

The GDPR holds several changes, including privacy by design and by default, informed consent and a larger scope of the GDPR in general,[2] to the previous Data Protection Directive,[3] which impacts businesses. The GDPR forces companies to think about their marketing statements and privacy policies and to inform their consumers about this. In particular, when health data is being processed, extra caution should be taken. These companies have a responsibility towards their consumers to protect their data and to inform them in an intelligible and easily accessible form of what data are being processed, why it is being processed and by whom.

This research examines to what extent discrepancies exist, if any, between the marketing statements vis-à-vis the actual privacy policies of three companies which process health data. It will then match these privacy policies against the GDPR and discuss possible legal consequences of discrepancies for both individuals and companies in light of the GDPR. It will do this in particular from a modern technologies and cross-border perspective. The outcome of this analysis will be used to conclude whether these companies sufficiently comply with the provisions of the GDPR and to determine whether the GDPR sufficiently reflects practical reality.

For this research, we analysed the privacy policies of three companies who offer apps and wearables that process health data. For the purpose of this article, namely to compare the privacy policies to the provisions of the GDPR, we decided to pseudonymise the names of the companies. This article focusses on the comparison and is not meant to name and shame these three companies. Especially considering that other companies more or less follow the same practices, which is discussed in more detail in the article 'Health apps, their privacy policies and the GDPR'.[4] For our article, we selected three companies, the apps of which serve a different purpose, while still being closely linked.

The first company (hereinafter: company A) specialises in activity trackers, but also offers the possibility to use their app without an activity tracker. In that case, the app simply uses the sensors of someone's mobile phone. This company traditionally focuses on wearables and therefore continuously collects data on the user's physical health. The second company (hereinafter: company B) focuses on measuring someone's running or cycling data and sharing of these data with friends. The third company (hereinafter:

[2]Articles 25, 4 (11) and 3 GDPR.

[3]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[4]T Mulder, 'Health apps, their privacy policies and the GDPR' (2019) 20 EJLT. This article analyses the privacy policies of 31 apps that process health data.

company C) focuses on mental health and stress reduction via meditation. The latter two companies only collect data when the app is used and focus on their users' physical health and mental health respectively.[5]

Processing health data

In our rapidly evolving digital world, technologies, including smart phones, wearables, virtual reality devices, self-driving vehicles, smart cities, smart maps, smart mirrors, etc., are advancing by the minute.[6] In healthcare in particular rapid digitisation and innovation is taking place by using the latest technologies, such as sensors, electrodes and other electronic devices.[7] Outside the medical context,[8] people use all sorts of modern technologies to track and measure their health and fitness, get into shape, keep fit, lose weight, reduce stress, etc. These technologies include for example mobile apps and wearables, such as watches and bracelets; but also smart fashion, such as glasses and clothing. These technologies enable people to monitor their own health and fitness by using (pressure) sensing technologies, which measure vital signs (such as heartrate) and track progress (such as counting steps).[9] New health technologies are a key area of the twenty-first-century knowledge societies and economies, offering the potential for growth and economic development.[10] It is one of the largest growing global markets. However, can the data processed by these health apps and wearables considered to be health data within the meaning of the GDPR?

When examining the privacy policies of the three selected companies it turns out that these companies have a different approach as regards the type of data collected from users. Company C does not mention that they collect health data, which lets to believe they think the data they process is not health data. Both companies A and B do mention the fact that they collect health data and even mention that explicit consent will be asked before a user can upload that type of sensitive data to the company.[11] There are two major legal frameworks which regulate data protection, namely the GDPR as well as the Council of Europe's Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Modernised Convention 108).[12] Convention 108 dates back to 1982 and has a larger reach than the GDPR considering

[5]In this article, we will discuss the highlights of what struck us when examining the privacy policies of these companies. Considering that we pseudonymised the names of the companies we did not include to this article our data set containing an extensive overview of the privacy policies' provisions compared to the GDPR.

[6]For example: <https://www.theguardian.com/technology/self-driving-cars> and <https://www.tno.nl/nl/aandachtsgebieden/mobiliteit-logistiek/roadmaps/smart-traffic-and-transport/smart-vehicles/> accessed 2 July 2019.

[7]For example: <https://ec.europa.eu/digital-single-market/en/news/mirror-mirror-wall-who-healthiest-them-all> and <https://ec.europa.eu/digital-single-market/en/news/do-you-drink-enough-ask-your-shirt-do-you-eat-too-much-ask-your-glasses> accessed 2 July 2019.

[8]We distinguish the processing of health data inside and outside the medical context. Inside the medical context is the processing of health data within a doctor-patient relationship, when the medical or healthcare professional is bound by professional secrecy and the technologies are used to treat patients. Outside the medical context is the processing of health data of consumers using modern technologies offered by companies. For the purpose of this research, we only discuss processing of health data outside the medical context.

[9]B Millington, 'Smartphone Apps and the Mobile Privatization of Health and Fitness' (2014) 31(5) CSMC 479.

[10]ML Flear and others, *European Law and New Health Technologies* (Oxford: University Press 2013) 1.

[11]For privacy reasons, we did not install and use these apps in order to investigate how this additional explicit consent is actually designed and what it exactly entails.

[12]Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf(2018)15-final).

that non-European countries can also become a State Party to the Convention. Both legal frameworks more or less follow the same logic.[13] They both provide for definitions of *personal data* and *health data* and determine that health data is a *special category of data*, also referred to as *sensitive data*.[14]

Both legal frameworks define personal data as *any information that can identify or help to identify a person*.[15] According to this definition, data that directly or indirectly[16] identifies an individual are considered to be personal data. Personal data are considered to be sensitive data when the type of data is more likely to impact the fundamental rights and freedoms of individuals.[17] Health data are unsurprisingly, considered to be sensitive data considering that this information can reveal a lot about a person.[18] There is some debate about the scope of the term *health data*. In this paper, we use the more common (overarching) term *health data*. The GDPR however uses the term *data concerning health,* meaning personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status. The Modernised Convention 108 uses the term *personal data for the information they reveal relating to health*.[19] According to the Explanatory report to the Modernised Convention 108 this includes information concerning the past, present and future physical or mental health of an individual and which may refer to a person who is sick or healthy.[20]

These EU and Council of Europe definitions are very broad. Personal data are considered to be health data as soon as it reveals information about a persons' health. The preamble to the GDPR provides some practical examples of what is covered by the definition of health data. It includes, among other things, information on a disease, a disability and even a disease risk. This means that information about a person's obesity, high or low blood pressure, genetic predisposition, but also information on tobacco consumption are part of health data since all these examples are linked to a disease risk of a person.[21] The preamble furthermore adds that it does not matter what the source of the information on a disease, a disability and a disease risk is.[22] This means that the source of the information is not limited to medical devices. As a consequence, information processed by commercial apps or wearables are therefore also part of this category of sensitive data.

[13]The focus of this paper will be on the GDPR; however, where relevant we will also refer to the Modernised Convention 108.

[14]Both the EU and the Council of Europe data protection legal frameworks were updated in 2018 after a lengthy reform/modernisation period.

[15]Article 4 (1) GDPR; Article 2 (a) Modernised Convention 108.

[16]Indirectly meaning that data, which relates to an individual, but not necessarily immediately identifies the individual is also considered to be personal data. By combining the data with other sources, an individual can still be identified.

[17]Recital 51 GDPR; Recital 55 Explanatory Report Modernised Convention 108.

[18]T Weichert, ABIDA report 'Big Data im Gesundheitsbereich' <http://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf> accessed 2 July 2019, p. 10. Medical confidentiality has long prohibited a medical professional to disclose information about a patient's case. This old obligation dates back to ancient Greece and is also known as the Hippocratic Oath. This is why it was the health sector that pushed for data protection regulation when modern technologies started to emerge.

[19]Article 4 (15) GDPR; Article 6 Modernised Convention 108.

[20]Council of Europe, 'Explanatory report to the Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data' (CETS No 223), para. 60.

[21]Recital 35 GDPR. For example, smoking increases the risk of lung cancer, a high blood pressure could indicate a heart problem and genetic predisposition could reveal risks on future diseases. See also para. 60 of the Explanatory Report to the Protocol amending Convention 108.

[22]Recital 35 GDPR.

According to the Article 29 Working Party,[23] in their 2015 'Annex – health data in apps and devices', personal data are health data when (1) the data are clearly medical data, (2) the data are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person or (3) conclusions are drawn about a person's health status or health risk.[24] This means that, most of the time, data are only health data when they are used or can be used to draw conclusions about a person's health. However, the Article 29 Working Party also acknowledges that in some cases the raw data itself are considered to be health data. For this article, we use that acknowledgement as a starting point. We consider raw data generated by health apps and wearables, which measure (mental) health and general fitness to be health data.

Considering this, the data generated by the three selected companies can be considered health data because they can reveal information about a person's (mental) health status. Companies A and B recognise the fact that they process health data, while company C does not mention this at all. In our opinion, the data collected by company C are also health data considering that they can reveal information about a person's mental health. We requested a copy of the personal data collected on one of our accounts. It turned out that company C, among other things, keeps track of how often you use the app and which packs you use. These packs, in particular the ones named *stress* or *anxiety* or *sadness*, combined with the frequency with which you use the app can say something about your mental health.

Considering the fact that all three apps process personal data, including health data, they need to comply with the provisions of the GDPR, including the provisions on sensitive data. First and foremost, the companies need to obtain explicit consent from their users to be able to process health data.

Consent

One of the principles for processing personal data is that the processing needs to be lawful, fair and transparent.[25] For lawfulness of processing, the GDPR determines that there are six legal grounds for processing, consent given by the data subject being one of them.[26] If there is no legal ground for processing, processing is considered to be unlawful. This is why most health apps and wearables have extensive privacy policies, which explain what data are collected, how these data are used and with whom the data are shared. A privacy policy is the most common way to inform people on how their data are going to be processed.[27] However, despite the information in the privacy policies, research showed that many people do not know that the data are used to target their behaviour and to what extent this is being done.[28] This cannot come as a real surprise, since research going back to 2008 has shown that a vast majority of people never read

[23]With the entry into force of the GDPR the Article 29 Working Party became the European Data Protection Board (EDPB).
[24]Article 29 Working Party (A29WP), Annex by letter – health data in apps and device, 2015 p. 5.
[25]According to Article 5 (1, a) GDPR and Article 5 (3) and (4, a) Modernised Convention 108.
[26]Article 6 (a) GDPR.
[27]L Hutton and T Henderson, 'Beyond the EULA: Improving Consent for Data Mining' (2017) TDM 146.
[28]B. Ur and others, 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising' Proc. 8th Symp. Usable Privacy and Security 2012.

privacy policies.[29] Since then, not a lot has changed.[30] Most people formally consent to privacy policies without knowing what happens to their personal data in practise.[31] This odd situation is called the privacy paradox: while people highly value their fundamental right to privacy, they do not act accordingly, especially when it concerns modern technologies.[32] Interestingly enough, both European legislators still decided to keep the explicit or informed consent exception for processing sensitive health data in their documents.[33] This creates an important task for the supervisory authorities to make sure companies at least comply with the demands of the GDPR on this point.

The GDPR protects the processing of sensitive data by, in principle, prohibiting such processing, unless one of the exemptions mentioned in Article 9 GDPR apply *and* suitable safeguards, to protect the data, are put in place. Suitable safeguards include, according to Article 32 GDPR, pseudonymisation and encryption. All three privacy policies elaborate on the way they keep the collected personal data safe. Both companies A and B mention encryption as a way to do this. They also both warn the user that no system is 100% safe and that they can give no guarantees on this matter. Company C does not mention encryption in their privacy policy, but does mention they follow *generally accepted standards* to keep the personal data protected and they offer the possibility to contact them if the user has any questions on this matter, as does company A. Although it is not possible for us to conclude that the three companies have suitable safeguards in place, it is clear that they have taken measures and want to inform the user about this to a certain degree.

Derogating from the prohibition to process special categories of personal data, including health data, is allowed when the data subject gives explicit consent. This means that the GDPR allows processing of personal data when a data subject explicitly consents. Consent of the data subject within the meaning of the GDPR means a clear affirmative act establishing at least the freely given, informed indication that the data subject agrees to the processing of his or her personal data.[34] The GDPR and Modernised Convention 108 do not determine how consent has to be given, which means that a data subject can give consent via, for example, a written statement, including by electronic means, or an oral statement.[35] However, if the data subject needs to give consent by electronic means, the request for consent has to be clear, concise and not unnecessarily disruptive.[36] This type of consent can be given for example by ticking a box when visiting a website, choosing certain technical settings or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing. Pre-ticked boxes or inactivity by the data subject do not constitute consent.[37] Furthermore, the request for consent needs to be presented in a clearly distinguishable form. This means

[29]AM McDonald and LF Cranor, 'The Cost of Reading Privacy Policies' (2008) JLPPIS.
[30]F Schaub and others, 'Designing Effective Privacy Notices and Controls' (2017) 99 IEEE IC.
[31]F Zuiderveen Borgesius, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13(2) IEEE S&P <DOI: 10.1109/MSP.2015.34> accessed 2 July 2019.
[32]M Taddicken, 'The "Privacy Paradox" in the Social Web' (2013) 19 JCMC.
[33]Article 9 (2, a) GDPR; Article 5 (2) Modernised Convention 108.
[34]Article 4 (11) GDPR and Article 5 (2) Modernised Convention 108.
[35]L Golba, 'Consent for Personal Data Processing in Digital Environment According to GDPR' (2017) 17(2) AAL 253 <https://www.humanitas.edu.pl/resources/upload/dokumenty/Wydawnictwo/Roczniki%20AiP%20-%20pliki/Podzielone/Roczniki%20AiP%202017%20z2/RAiP_2_2017-253-265.pdf> accessed 2 July 2019.
[36]Article 7 (1) GDPR.
[37]Recital 32 GDPR.

that it cannot be buried within a contract or other written document. Where processing is based on consent, Article 7 GDPR determines that the controller needs to be able to demonstrate that the data subject has given consent to the processing activities and makes it possible for the data subject to withdraw his or her consent at any time in a way that is just as easy, or difficult, as it was to give the consent in the first place.[38] This means that an app company needs to think about how to request consent in a manner that complies with the GDPR and how to demonstrate this to the supervisory authority upon request.[39]

The question rises what *freely given and informed* entails within the notion of consent. Freely given consent means that the data subject has a genuine or free choice or is able to refuse or withdraw consent without detriment.[40] For consent to be informed, the data subject needs to be aware of the identity of the controller and the purpose of processing.[41] All three privacy policies provide the user with the identity of the controller. However, the purposes for processing are in all three policies vague. Both companies A and B mention that they use the data to 'provide and maintain' or 'analyze, develop and improve' services and mention examples such as 'troubleshoot and protect against errors', 'develop new features and Services' or 'provide you with statistics and visualizations representing key data points like heart rate'. Unfortunately, both companies also only mention these examples as examples, what leads to believe they also use this information in other situations. Company C seems to be more complete, since it seems to sum up all the ways they use a costumer's personal data. They do, however, also mention in one of the cases that they use

> details of your visits to and interactions with the Products including, but not limited to, traffic data, location data, weblogs and other communication data, whether this is required for our own billing purposes *or otherwise* and the resources that you access.

Especially adding 'or otherwise' makes it quite unclear for what purposes these kind of highly sensitive data are used. If it is not clear what the purposes for the processing are exactly, we have to conclude that the consent is not informed and therefore the processing unlawful. One could argue that the user has the possibility to actively exercise their right of access to get a complete overview of the purposes of processing. All three companies offer this possibility, but exercising this right is in hindsight, while consent is given in advance. This option therefore does not correct the wrong. In our view a proactive role in this regard of supervisory authorities could stimulate companies to be more open and concrete about their purposes for processing.

Clear and plain language

Another condition for consent is that the written declaration, in this case the privacy policy, is written in a clear and plain language.[42] This is also a general requirement for

[38]E Politou and others, 'Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions' (2018) 1(20) JC <DOI 10.1093/cybsec/tyy001> accesses 2 July 2019.
[39]See for example: HJ Pandit and others, 'GDPR-driven Change Detection in Consent and Activity Metadata' (2018) 2112 CEUR Workshop Proceedings 16.
[40]Recital 42 GDPR.
[41]Ibid.
[42]Article 7 (2) GDPR.

transparency, which we will discuss in the following paragraph. It is remarkable that all three privacy policies start by mentioning how important they believe the users' privacy is. For this they turn to the reader personally and use terms such as '[we are] committed to protecting and respecting your privacy' or 'your privacy is very important to us' and 'we appreciate that you are trusting us with information that is important to you, and we want to be transparent about how we use it'. Although we are not experts in the field of psychology, and we do not aim to be, it strikes us that all three privacy policies address the reader directly and all three give the impression that they think the readers' privacy is important to the reader and therefore also to them.

What follows, also in all three cases, is quite a lengthy text varying between 3500 and 4000 words. On average, a person reads 200–250 words per minute, which means that these privacy policies will take about 15–20 min each to read. Two out of three privacy policies are written in English, one is written in the local language, in our case Dutch. Even though it might make it easier for some people to read a privacy policy in their own language, the concerned privacy policy states that the English version of the privacy policy takes precedence when the translated version conflicts with the English version. This would suggest that the Dutch reader can also easily find the English version of the privacy policy, since that version takes precedence. However, strangely enough, this is not the case. There is no link to the English version of the privacy policy and the user will have to adjust their computer settings to English before being able to read the controlling English version. Although the idea of offering the text of the privacy policy in someone's own language might by user friendly, the actual implementation in this case is questionable since a user has to go through a lot of trouble to find the controlling English version. Since transparency is a key element of the GDPR, it is very much the question whether this solution meets the requirements.[43]

Transparency

According to Articles 5 (1, a) and 12 GDPR personal data needs to be processed in a transparent manner.[44] Companies need to be transparent about the information referred to in Articles 13 and 14, the rights of the data subject in Articles 15–22 and communication of a data breach if it occurs (Article 34). This information needs to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[45] The idea behind transparency is that organisations and companies gather a large amount of data from people in order to provide services or to sell products. These data can tell these organisations and companies a lot about a person. Persons thus give up some of their privacy in order to receive the services or purchase the goods. This is why processing personal data needs to be lawful and fair and why the GDPR provides persons with rights. In order to exercise these rights, persons need to know what data concerning them are collected, used, consulted or otherwise processed. This is referred to as the principle of transparency. A person needs to know who processes the data, what the purpose of processing is, what the risks, rules, safeguards and rights are and how to exercise them. We

[43]Article 12 GDPR and Ibid (n. 41).
[44]Article 5 (1, a) GDPR.
[45]Y McDermott, 'Conceptualising the Right to Data Protection in an Era of Big Data' (2017) BD&S <DOI: 10.1177/2053951716686994> accessed 2 July 2019. As regards the clear and plain language, see also the paragraph above.

compared the texts of the privacy policies of the three selected companies with the GDPR in order to conclude whether the companies comply with the transparency rules of the GDPR. The most relevant and striking conclusions will be discussed below.

The three selected companies collect personal data directly from their users. As such, they need to provide data subjects with the information mentioned in Article 13 GDPR in order to be transparent. In their privacy policies, all three companies provide the user with their identity and contact details. The question *who processes the data* is therefore clear. However, data can also be shared with third parties. All three privacy policies mention several categories of recipients, such as corporate affiliates, service providers and partners. These parties are not actually named, which leaves the door open to share data with a variety of unknown parties considering that the categories are very broad. When it comes to *why the data are being processed,* one of the privacy policies does not mention a legal basis for processing, while the other two mention several possible legal bases, but do not link this to the collected data. Another important question is where the data are being processed. Two privacy policies mention that they process data in the United States (US), the third one mentions *the United States and other countries*. This means that the data in all three cases cross the EU border. Cross-border challenges will be discussed in the next paragraph. The fact that both the purpose of processing as well as the recipients and countries the data are shared with remains vague means that there is a lot of room for interpretation. In our view, this cannot be considered transparency within the meaning of the GDPR.

Companies furthermore need to inform users about their rights under Articles 15–22 GDPR and facilitate the exercise of these rights. One of the most important rights for data subjects is the *right to request access* to the data that are collected about them. All three privacy policies offer data subjects the possibility to request access to their data, however, what is striking is that two out of the three policies offer this only to data subjects who live in the EU or rather in the European Economic Area (EEA), the United Kingdom (UK), and Switzerland. These two policies furthermore also only offer the possibility to access *much of your personal data via your account,* which suggests that users cannot access all of their personal data. The same goes for another important right, the *right to be forgotten* (the right to request erasure). Only one privacy policy offers this option to everyone around the globe while the other two only give this option to data subjects in the EU, EEA, UK and Switzerland. No doubt these two examples are a consequence of the entry into force of the GDPR. Data subjects outside the EU thus appear to have less rights and therefore less protection. Unfortunately, the US are only observers to Modernised Convention 108 and not a State Party. This means that the rights described in Article 9 Modernised Convention 108 do not apply in the US.

Data subjects also need to be made aware of the fact that they can exercise their rights. One way to exercise rights is to contact the designated Data Protection Officer (DPO) with regard to all issues related to the processing of their personal data. Only one of the companies however provides the e-mail address of their DPO in the privacy policy.[46]

[46] According to Article 37 GDPR, a Data Protection Officer (DPO) needs to be appointed if the core activities of a controller or processor consist of processing on a large scale of special categories of data. *Core activities*, according to the Article 29 Working Party are the key operations to achieve the controller's or processor's goals. Processing data are the key operations of the three selected companies considering that this is necessary in order to count the amount of steps a user takes, track the time cycled or meditated, etc. Determining whether processing takes place *on a large scale* depends,

Another way to do exercise rights is to lodge a complaint with a supervisory authority and to seek a judicial remedy. Controllers need to inform data subjects of this possibility if they do not take action on requests of data subjects in the exercise of their rights under Articles 15–22 GDPR. Two out of three privacy policies mention the possibility to lodge a complaint with a supervisory authority. The third one mentions the possibility to file a complaint under the Privacy Shield Framework. Considering the fact that people often do not read privacy policies and the privacy policies are not always clear about their processing activities, it is in our opinion a task of the supervisory authorities to monitor compliance with the GDPR and help protect the rights and freedoms of data subjects. This is important because cross-border exercise of rights can be very difficult for individual data subjects.

Finally, in case of a health data breach which is likely to result in a high risk to the rights and freedoms of persons, data subjects need to be informed of this data breach without undue delay following Article 34 GDPR. According to Article 4 (12) GDPR a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Inherent to data breaches is that a breach is not necessarily contained to one country, in particular when data subjects all over the globe use modern technologies, such as apps and wearables. When it comes to health data breaches, there are various risks, including for example the risk of health data being used or sold for a commercial aim. The health sector is one of the most affected sectors: in the first quarter of 2018 1.13 million patient records were breached via 110 data breaches.[47] These breaches where mainly caused by snooping on family members, neighbours and VIPs and by hacking incidents. Most of these health data records can be found and bought online via illegal market places. While these breaches are clearly inside medical context, one can assume that health data generated by modern technologies outside medical context can also be used for malicious purposes. There are unfortunately no numbers available on data breaches within companies, most likely considering that companies not always publish their major breaches for reputational reasons. According to the GDPR companies only need to notify the supervisory authority and communicate the data breach to the data subject in case of a high risk to rights and freedoms.[48] When health data is involved in a data breach, damages are likely to occur, meaning that there is a high risk to rights and freedoms. The 2018 Strava and Polar incidents[49] are indicators that data breaches do exist in the private sector. These were major incidents, which became publicly known. We can only

among other things, on the number of data subjects concerned and the geographical extent of the processing activities. All three companies offer their apps and wearables around the globe and have over 10 million downloads on android devices alone, not including iOS and Windows devices, which can be considered as processing on a large scale. See Article 29 Working Party, Guidelines on Data Protection Officers (DPO's), WP 243 rev.01, p. 7, 8. It can therefore be concluded that all three companies require the designation of a DPO.

[47] <https://protenus.com/press/press-release/113m-patient-records-breached-from-january-to-march-2018> accessed 2 July.

[48] Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, p. 23.

[49] See for example <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases> and M Martijn and others, 'This Fitness App Lets Anyone find Names and Addresses for Thousands of Soldiers and Secret Agents' [2018] <https://decorrespondent.nl/8480/this-fitness-app-lets-anyone-find-names-and-addresses-for-thousands-of-soldiers-and-secret-agents/260810880-cc840165> accessed 2 July 2019.

assume that this happens more often than we hear about considering that companies are not obliged to make their data breaches public.

Crossing borders

Finally, also inherent to modern technologies is that data are not limited to countries' borders. Data can be transferred and stored anywhere in the world. Offering a similar level of protection within the EU is one of the reasons why the GDPR was created. However, when personal data moves across borders outside the EU, there is an increased risk to maintain the high level of protection offered by the GDPR. It might be, for example, more difficult for people to exercise their data protection rights.[50] This is why the GDPR provides for strict rules for transfer of data outside the EU. In this paragraph, we will look into cross-border health data flows.

Technology transformed both the economy and social life.[51] People increasingly make personal information available publicly and globally by using modern technologies. Due to the very nature of these technologies, data are not necessarily bound by country or EU borders. How the health data flows inside medical context, although it may vary depending on the healthcare systems of countries, is pretty clear.[52] Outside the medical context however, in particular when speaking about modern technologies, it is more difficult to determine how health data flows. One of the consequences of the electronic capturing of personal data via modern technologies is that, due to the very nature of these modern technologies, data may be located and stored anywhere in the world. In general, as also follows from the analysed privacy policies, health data processed by modern technologies are transferred from the device (such as a smartphone or wearable), which records these data, to a cloud and/or to the servers of the companies.[53] Once these data are in the cloud and/or on the servers of the companies, it becomes more difficult to trace how these data flow. According to the analysed privacy policies, the data can be shared with *corporate affiliates, service providers and other partners* (the parties) in the US and *other countries* around the world. It is however not clear who these parties are, where they are based, which data exactly are shared and how these data are shared, i.e. whether access to these data are granted to the cloud/servers or whether these data are transferred to the parties. If these data are actually transferred to the parties, it becomes even more difficult to trace. It can be presumed that in such cases, the data are then stored on the cloud/servers of these parties, the location of which is unknown to the data subject. These parties furthermore may or may not share these data with third parties of their own. These practices by companies are vague and unclear, i.e. not transparent. While responsibility to protect the data of

[50] In the privacy policies we analysed for this paper we found two examples of this: … *you acknowledge and understand that your information will be transferred, processed and stored in the United States (…) United States privacy laws may not be as protective as those in your jurisdiction* and *Please note that the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country*.

[51] S Fisher-Hubner and others, 'How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used?' (2013) PIMEST 77.

[52] Inside the medical context, health data is shared in a closed circuit, for example, between medical and healthcare professionals and insurance companies to provide patients with healthcare.

[53] Although the cloud consists of servers, not every server is a cloud. See for example: N Robinson and others, 'The Cloud, Understanding the Security, Privacy and Trust Challenges' (2010) RAND Corporation 17.

their users remains with the original controllers, there are a number of challenges with these practices.

The increase in data flows raises challenges and concerns as regards the protection of personal data, especially if data flows to and from countries outside the EU. Therefore, Article 3 determines that the GDPR applies to processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU if the processing activities relate to offering goods or services or monitoring the behaviour of data subjects. The aim of the GDPR is to offer a similar level of protection for EU citizens regardless of whether the data are being processed inside or outside the EU.[54] This means that the GDPR, including the additional protection rules for sensitive data, also applies to companies established outside the EU if they are processing personal data of data subjects within the EU. Companies processing health data, whether or not established in the EU, thus need to comply with the GDPR.

The first question that rises is whether transfer from the device, which records the data to the cloud/server, is transfer within the meaning of Chapter V of the GDPR and is as such protected. It is unclear whether the device functions only as a tool for the companies to collect data and if the transfer to the cloud/server can be seen as a mere transit rather than transfer within the meaning of the GDPR.[55] The major challenge here is, however, that privacy policies are unclear about the parties and countries they share data with. First of all, as a result of this, there is a lack of transparency as regards the use, location and storage of the data. This makes the data difficult to trace, i.e. who has which data, what do they use the data for and where are the data stored. Secondly, and more importantly, this makes it difficult to determine jurisdiction and thus difficult for data subjects to exercise their rights in case of an infringement of rights and freedoms. Even though the GDPR determines that its territorial scope reaches across the globe when personal data of data subjects who are in the EU are being processed, the actual exercise of rights is more difficult.[56] Not only physically, but also considering that legal systems in third (non-EU) countries may not recognise or may not have knowledge of the GDPR.[57]

The question of jurisdiction is probably one of the reasons the GDPR has a chapter on the transfer of personal data to third countries or international organisations.[58] The general principle in Article 44 GDPR is that data cannot be transferred to a third country unless the conditions of Chapter V are met. According to Article 45 GDPR

[54]N Daśko, 'The General Data Protection Regulation (GDPR) – A Revolution Coming of European Data Protection Laws in 2018. What's New for Ordinary Citizens?' CLR 128 <https://doi.org/10.12775/CLR.2017.005> accessed 2 July 2019.

[55]See for example: The concept of 'transfer' of data under European data protection law – in the context of transborder data flows, Faculty of Law – University of Oslo [2015] <https://www.duo.uio.no/bitstream/handle/10852/49722/8026_The-concept-of-transfer-of-data-under-European-data-protection-law---In-the-context-of-transborder-data-flows.pdf?sequence=1&isAllowed=y> accessed 2 July 2019. Going into this discussion would result in a paper in itself, and it is therefore outside the scope of this paper to discuss this further.

[56]One major criticism is that territorial scope can be limiting and problematic in today's world where electronic information is processed, shared and stored across several territorial jurisdictions and spaces. This is why in other areas, such as law enforcement, debate is taking place on whether it is time for jurisdiction to change. In law enforcement there is mention of universal or investigative jurisdiction, see for example: D.J.B. Svantesson, 'Law Enforcement Cross-border Access to Data', *Preliminary Report* November 2016; D.J.B. Svantesson and L. van Zwieten, 'Law Enforcement Access to Evidence via Direct Contact with Cloud Providers – Identifying the Contours of a Solution' (2016) 32 Computer Law & Security Review 671. An analogy can perhaps be made here as regards supervisory authorities.

[57]See for example A McQuinn and D Castro, 'How Law Enforcement Should Access Data across Borders' (2017) IT&IF 30.

[58]Chapter V GDPR.

transfer to a third country can take place if there is an adequacy decision. The EU – US Privacy Shield is an example of such an adequacy decision. Considering that all three companies process personal data of European citizens in the US, the EU – US Privacy Shield can apply. This framework became operational on 1 August 2016 and claims to protect *the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes*.[59] Companies A and C have joined this programme and therefore refer to it in their privacy policies. The privacy policy of company B does, however, not mention the programme. Further investigation shows that company B did not join the programme, meaning that they cannot rely on the Privacy Shield framework.[60] Therefore, company C has to comply with Article 49 GDPR, which states that in the absence of an adequacy decision data can still be transferred to a third country if the data subject has explicitly consented to the transfer, after having been informed of the possible risks of this transfer 'due to the absence of an adequacy decision and appropriate safeguards'.[61] Although company B mentions that privacy laws in the US might be less protective, there is no mention of the absence of an adequacy decision and also no information on the possible risks, not even an example. This means that company B is not allowed to transfer the data outside of the EU. However, they still transfer personal data outside of the EU. In our opinion there is, again, a role for supervisory authorities to stimulate international companies to comply with the GDPR.

Conclusion

This research showed that there is a gap between data protection laws in Europe and practical reality. After comparing the privacy policies of three commercial health apps and wearables to the provisions of the GDPR we can conclude that these privacy policies are unclear about the processing activities in general. It is the responsibility of these companies to protect their users' privacy. While at first glance the policies seem to be well-drafted and the marketing statement gives the impression that privacy is important, a careful analysis of these three policies showed that they are vague about the purposes for processing, how much personal health data are processed, where in the world the data are processed and with whom the data are shared. Taking this into account, linked with the fact that people often do not read privacy policies and/or choose convenience over privacy, it is in our opinion a task for the supervisory authorities to monitor compliance of these companies to the GDPR. This can be done by a cooperation between national and European supervisory authorities. However, the challenges cannot only be addressed by legal means and enforcement thereof by supervisory authorities. It is also very much a societal challenge, which could be addressed by societal organisations (such as patient organisations, consumers associations, etc.) via various campaigns. This way the protection of fundamental rights and freedoms of individuals with regard to cross-border processing of health data can truly be achieved.

[59] <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en> accessed 2 July 2019.
[60] <https://www.privacyshield.gov/participant_search> accessed 2 July 2019.
[61] Article 49 (1, a) GDPR.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

T. Mulder http://orcid.org/0000-0003-2056-5140