The mHealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union

Hannah van Kolfschooten[*]

An increasing number of EU citizens uses self-monitoring mHealth apps: apps used by consumers in a private setting to monitor their general health. The extensive processing of health data by these apps poses severe risks to users' privacy. These risks are exacerbated by the inapplicability of the EU legal framework on health and patients' rights to these apps. Furthermore, while the EU's General Data Protection Regulation provides a solid legal framework for the protection of health data, in practice, many mHealth apps do not comply. In light of the lack of effective EU regulation, this paper examines the feasibility of self-regulation by app stores as a complementary form of regulation in order to improve the level of protection of EU mHealth app users. App stores already play an important role by regulating third-party mHealth apps distributed on their platforms in a top-down manner by means of app review procedures. In order to assess the effectiveness of these existing practices, a case study analysis is performed on the regulatory practices of Apple's App Store and Google's Google Play Store. This analysis is the basis for recommendations on how to strengthen current self-regulation initiatives by app stores in the context of health data protection.

1. Introduction: mHealth Apps: Promise or Threat?

An increasing number of European Union (EU) citizens use mobile apps to monitor their own fitness, lifestyle or general health to take control over their own health outside of a clinical setting.[1] This growing trend is reflected in the content of mobile app stores: self-monitoring mobile health (mHealth) apps such as running trackers and medication reminders are omnipresent. While mHealth apps are said to hold great potential for empowering individuals, the apps also constitute threats to users' fundamental rights in the EU.[2] The main risk is posed by the extensive processing and sharing of health data with third-parties by mHealth apps. Users have limited awareness of, and control over, who has access to their

[*] PhD researcher and lecturer at the Law Center for Health and Life, University of Amsterdam.

[1] INCISIVE HEALTH INTERNATIONAL, *Taking the pulse of eHealth in the EU An analysis of public attitudes to eHealth issues in Austria, Bulgaria, Estonia, France, Germany, Italy, and the UK* (2017).

[2] EUROPEAN COMMISSION, *GREEN PAPER on mobile Health ("mHealth") {SWD(2014) 135 final}*.

health data.[3] This leads to a paradox: users turn to mHealth to increase self-empowerment, but at the same time surrender power due to this lack of data control.[4]

These risks are further compounded by the lack of effective EU regulation. The EU legal framework on health and protection of patients' rights does not apply to self-monitoring mHealth app users.[5] Furthermore, while the EU's General Data Protection Regulation (GDPR) provides a solid legal framework for the protection of health data, in practice, many mHealth apps do not comply with its provisions.[6] When traditional legislative regulation does not lead to the intended effect, complementary alternative forms of regulation may be the solution.[7] In the context of health data protection in mHealth apps, mobile app distribution platforms (app stores) may be well-positioned to improve health data protection by means of self-regulation. App stores in the EU already occupy an important place in this regard by offering a top-down regulation of third-party mHealth apps distributed on their platforms by means of app review procedures. App stores require app developers to comply with certain rules as part of a preapproval process and remove non-compliant apps. This "gatekeeping function" empowers app stores to influence app developers' conduct: a form of industry self-regulation.[8] Starting from this premise, the purpose of this article is to evaluate whether and to what extent self-regulation by app stores may contribute to the level of health data protection in the EU.

The article is structured as follows. First, it outlines health data protection issues concerning mHealth apps (section 2). Next, it describes the EU legal framework governing mHealth apps, focussing on the GDPR (section 3). Subsequently, it discusses the benefits and risks of industry self-regulation as an alternative means to protect data protection rights in light of current mHealth regulation practices by Apple's App Store and Google's Google Play (section 4). Finally, this chapter proposes several improvements to self-regulation in this field (section 5), which will provide the basis for conclusions (section 6).

2. Health Privacy Issues in Self-Monitoring mHealth Apps

Popular examples of mHealth apps include calorie counters, apps to monitor menstruation cycles and running trackers. These types of apps continuously monitor users' behaviour over an extended period of time. While the focus of mHealth apps ranges from health to fitness and lifestyle, all of them collect

---

[3] Keith Spiller et al., *Data Privacy: Users' Thoughts on Quantified Self Personal Data*, *in* SELF-TRACKING: EMPIRICAL AND PHILOSOPHICAL INVESTIGATIONS 111–124 (Btihaj Ajana ed., 2018).

[4] Federica Lucivero & Karin R. Jongsma, *A mobile revolution for healthcare? Setting the agenda for bioethics*, 44 JOURNAL OF MEDICAL ETHICS 685–689 (2018).

[5] COMMISSION STAFF WORKING DOCUMENT ON THE EXISTING EU LEGAL FRAMEWORK APPLICABLE TO LIFESTYLE AND WELLBEING APPS ACCOMPANYING THE DOCUMENT GREEN PAPER ON MOBILE HEALTH ("MHEALTH"), (2014). Also see Recital 19 of the MDR.

[6] Quinn Grundy et al., *Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis*, 364 BMJ l920 (2019); Achilleas Papageorgiou et al., *Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice*, PP IEEE ACCESS 1–1 (2018).

[7] Anil K. Gupta & Lawrence J. Lad, *Industry Self-Regulation: An Economic, Organizational, and Political Analysis*, 8 AMR 416–425 (1983).

[8] Adrian Fong, *The role of app intermediaries in protecting data privacy*, 25 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 85–114 (2017).

large amounts of health-related data, such as biometric data, data concerning vital body functions and health indicators. Most of these data qualifies as 'data concerning health' within the meaning of the GDPR.[9] Health data should be understood in a broad manner.[10] The GDPR's definition of health data implies that information about users' weight, blood pressure, tobacco and alcohol consumption is considered health data, because this information is scientifically linked to health or disease risks.[11] Furthermore, certain types of information may not be health data *as such*, but may transform into health data when monitoring takes place over a longer period of time (i.e. average steps per month), or the data is combined with other data sources (i.e. daily calorie intake and social media profile).[12]

The risk for a violation of the users' fundamental rights is high, since misuse of health data may be irreversible and have long-term effects on data subjects' lives and social environments.[13] Several studies show that the extensive processing of health data by mHealth apps poses numerous threats to privacy.[14] This is mainly caused by the fact that health data is valuable commodity: big data companies are increasingly interested in health data as it is scarce because of the expensive collection process.[15] Therefore, mHealth apps may encourage users to provide more health data in order to make more profit. Passively collected data, such as calculated overviews of average steps, are regularly collected beyond users' control.[16] Moreover, mHealth apps often use a standard Terms of Service, setting the rules on a 'take it or leave it' basis.[17] Consequently, users are often unaware of the exact type and volume of collected data.[18]

Additional concerns are raised with regard to the user's control over access to the collected health data. Most apps provide for the possibility to disclose information to an "undefined (future) audience".[19] For example, many apps share health data among unspecified users to provide comparisons and app operators may sell health data to third parties, such as advertisers and insurance companies.[20] Apps often do not provide the option to consent granularly: users have to consent to all receivers and all types of data at once.[21] In conclusion, the extensive processing and third-party sharing of health data by mHealth apps compromises users' control and therefore poses threats to users' privacy rights.

3. The Effectiveness of EU Legal Protection of Health data in mHealth Apps

[9] Recital 35 GDPR.
[10] ARTICLE 29 DATA PROTECTION WORKING PARTY, *ANNEX - health data in apps and devices* (2015) 2.
[11] *Id.*
[12] *Id, 3-5.*
[13] Z v Finland (1997) 25 Eur. Ct. H.R. 371, 94-96.
[14] See for an overview: Dominik Leibenger et al., *Privacy Challenges in the Quantified Self Movement – An EU Perspective*, 2016 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 315–334 (2016).
[15] Grazia Cecere, Fabrice Le Guel & Vincent Lefrere, *Economics of free mobile applications: Personal data as a monetization strategy* 45 (2018).
[16] Papageorgiou et al., *supra* note 6.
[17] *Id.*
[18] Kirsten Ostherr et al., *Trust and privacy in the context of user-generated health data*, 4 BIG DATA & SOCIETY (2017).
[19] Marjolein Lanzing, *The transparent self*, 18 ETHICS AND INFORMATION TECHNOLOGY 9–16 (2016).
[20] Leibenger et al., *supra* note 22.
[21] COMMISSION STAFF WORKING DOCUMENT, *supra* note 5.

3.1 Inapplicability of the EU Health Framework

In the EU, health privacy in technology is regulated via multiple legal instruments. At the national level, health privacy is protected through patients' rights frameworks. One basic right can be identified in all Member States: medical confidentiality. Medical confidentiality entails both the patient's right to confidentiality of personal data and the duty for health professionals to keep this data confidential.[22] However, mHealth app users are generally not considered patients by app developers nor in their own experience, as the apps do not serve a medical purpose and health professionals are not involved.[23] Therefore, users are not protected under the patients' rights framework.

At the EU level, health technology is mainly regulated through regulation of medical devices under the Medical Devices Regulation (MDR).[24] Software, including apps, may also fall under the MDR.[25] However, in order to qualify as medical device, the intended purpose of the app needs to fall within one of the medical purpose categories stipulated by the MDR.[26] As most self-monitoring mHealth apps (monitoring fitness, general health or wellbeing) are not intended for medical purposes but instead focus on general health, they usually do not qualify as medical devices.[27] The MDR specifically excludes software intended for general purposes and lifestyle and wellbeing purposes.[28] However, when apps do have an intended medical purpose, e.g. self-monitoring apps prescribed by a physician, the MDR may apply. In any case, the MDR protects health privacy primarily with reference to the GDPR.[29]

3.2 The GDPR Protects Health Data in Theory…

The main instrument for health privacy protection in the EU is the GDPR. The GDPR provides individuals with several rights concerning personal data processing.[30] The GDPR applies to mHealth apps available in the EU.[31] The basic premise of the GDPR is that every processing of personal data must be underpinned by a legal basis.[32] Moreover, it imposes duties on data processors and controllers and confers rights on data subjects in order to increase control.[33] Data subjects' rights include the right to information,[34] the right to access[35] and the right to withdraw consent.[36] Furthermore, the GDPR provides for a special data protection regime for health data, which stipulates a general prohibition on

---

[22] TAMARA K. HERVEY & JEAN V. MCHALE, EUROPEAN UNION HEALTH LAW (2015).
[23] COMMISSION STAFF WORKING DOCUMENT, *supra* note 5.
[24] NB: Regulation (EU) 2017/745 (MDR) will replace the current Directive 93/42/EEC in May 2020.
[25] CJEU, Case C-329/16 (*SNITEM).*
[26] See Helen Yu, Chapter X in I. Glenn Cohen, Timo Minssen, W. Nicholson Price II, Christopher Robertson, and Carmel Shachar. The Future of Medical Device Regulation: Innovation and Protection. Cambridge University Press, 2021.
[27] EUROPEAN COMMISSION, *Guidance document Medical Devices - Scope, field of application, definition - Qualification and Classification of stand alone software* (2016).
[28] Recital 19 MDR.
[29] Article 109 and 110 MDR.
[30] Recitals 7 and 63 GDPR.
[31] Articles 2 and 3 GDPR; EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 1/2015 Mobile Health: Reconciling technological innovation with data protection* (2015).
[32] Article 6 GDPR.
[33] Chapter III GDPR.
[34] Articles 12 and 13 GDPR.
[35] Article 15 GDPR.
[36] Article 7(3) GDPR.

the processing of health data but provides for limited derogations.[37] However, these derogations are arguably inapplicable to mHealth apps, because app developers do not process health data in the public interest[38] and are not bound by professional secrecy.[39] Therefore, typically, health data can only be processed in mHealth apps when users provide their *explicit* consent.[40] This implies that the data subject must give an "*express* statement of consent".[41] The GDPR's extensive protection of data rights in combination with the strict health data regime gives it the potential to sufficiently protect mHealth users' health data.

3.4 …But the GDPR Does Not Effectively Protect Health Data in Practice

However, several empirical studies show that many mHealth apps do not comply with relevant GDPR provisions related to health data.[42] For example, from a study on 20 mHealth apps available in the EU it was found that the majority of mHealth apps do not comply with provisions on user consent: 55% of the analysed apps provides information about the app provider's privacy policy before registration, only 5% asks for consent every time the user shares additional personal information, none of the apps comply with the requirement of expressing 'explicit' consent by specific questions or an online form and only 35% offers the possibility to withdraw consent and thereby delete their health data.[43] Another analysis of privacy policies of 31 EU mHealth apps shows that none complied with the right to information: only 42% mentioned the right to object and 58% the right to rectification and access.[44] A different study on 24 mHealth apps shows that 79% sends users' health data to third parties in a non-transparent manner.[45]

Thus, in practice, many mHealth apps do not seem to comply with the GDPR. This can be explained by the fact that apps are often developed by individuals located all over the world, with little understanding of applicable data protection legislation.[46] Furthermore, due to the great number of available apps, regulatory oversight is difficult because of insufficient resources.[47] The majority of Member States does not have an entity that is responsible for the regulatory oversight of mHealth apps.[48] Knowledge of lack of oversight may also result in lower compliance. In sum, the GDPR offers a relevant and sufficient legal framework for protection of health data but lack of compliance and enforcement

[37] Article 9 GDPR.
[38] Article 9(2)(b-j) GDPR.
[39] Article 9(3) GDPR.
[40] Article 9(2)(a) GDPR.
[41] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on consent under Regulation 2016/679* (2018) 18-19; Article 32 GDPR.
[42] See for overview: Grundy et al., *supra* note 6.
[43] Papageorgiou et al., *supra* note 6.
[44] Mulder, *supra* note 6.
[45] Grundy et al., *supra* note 6.
[46] Fong, *supra* note 13, 98.
[47] ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES, (David Wright & Paul De Hert eds., 2016), 29-31.
[48] CARRIE BETH PETERSON, CLAYTON HAMILTON & PER HASVOLD, FROM INNOVATION TO IMPLEMENTATION: EHEALTH IN THE WHO EUROPEAN REGION (2016).

make the GDPR a practically ineffective instrument to protect mHealth users. Therefore, as long as compliance is not strengthened, traditional legislative regulation does not suffice.

4. Self-Regulation by App Stores as a Solution to Improve Health Data Protection

When traditional (legislative) regulation does not lead to the intended effect, complementary alternative forms of regulation, such as self-regulation, may be the solution.[49] While the important role of app stores in securing GDPR compliance has been recognised by the EU on several occasions,[50] and the role of digital platforms in protecting fundamental rights online is a popular topic in legal scholarship, the discussion seems to focus mainly on social media platforms and does not elaborate on app stores.[51] However, app stores may be well-positioned to improve health data protection by means of self-regulation.

4.1 Self-Regulation in Data Protection

Industry self-regulation can be defined as "a regulatory process whereby an industry-level, as opposed to a governmental- or firm-level, organisation (…) sets and enforces rules and standards relating to the conduct of firms in the industry."[52] Often-mentioned benefits of self-regulation are flexibility in adapting rules to technological changes, greater quality of rules and more commitment to the rules.[53] However, self-regulation also has its limitations, specifically with regard to fundamental rights protection. Self-regulation instruments often lack effective enforcement and monitoring mechanisms. Furthermore, in some cases, self-regulation instruments are not consistent with other existing regulation, which makes the overall regulatory system increasingly complex. Other challenges include risks for favouritism and lack of accountability.[54]

In the context of data protection, self-regulation by the industry is becoming more common. Companies often choose to complement existing legislation with self-regulatory instruments for reasons of protecting consumer interests, increasing public trust and reputation and combatting negative public opinions.[55] Also, self-regulation has been given prominence in the context of data protection at the EU level: the GDPR supports and encourages self-regulation by businesses in the form of code of conducts and Binding Corporate Rules.[56] Moreover, the European Commission has (so far unsuccessfully) taken steps to set up a voluntary Privacy Code of Conduct on mHealth apps for app developers.[57]

---

[49] OECD, *supra* note 11, 4-7; Gupta and Lad, *supra* note 7, 417.
[50] EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Privacy and data protection in mobile applications* (2018), 16; ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 30, 11-12.
[51] See i.e. CHRISTINA ANGELOPOULOS ET AL., *Study of fundamental rights limitations for online enforcement through selfregulation* 96.
[52] Gupta and Lad, *supra* note 7, 417.
[53] Rebecca Ong, *Mobile communication and the protection of children*, 2010, 247-249.
[54] OECD, *supra* note 11, 6-7, 42.
[55] App Stores List (2019), BUSINESS OF APPS (2017), https://www.businessofapps.com/guide/app-stores-list/ (last visited Feb 24, 2020) 131-132.
[56] Art 40 and 47 GDPR.
[57] European Commission, *supra* note 10.

4.2 App Stores as Privacy Regulators

With regard to industry self-regulation of mHealth apps in the EU, we see that app stores already play an important role by top-down regulating third-party mHealth apps distributed on their platforms by means of app review procedures.[58] The app-ecosystem works as follows: in order for app developers to distribute their apps to the general public, they need to publish their app in app stores for consumers to download onto their mobile devices. App stores require app developers to comply with certain rules as part of a preapproval process and remove non-compliant apps. This 'gatekeeping function' empowers app stores to influence app developers' conduct.[59] Therefore, app stores are the central orchestrators in the app-ecosystem and have a large amount of control over consumers.[60]

App stores are not regulated under the GDPR. They do not qualify as data processors or controllers under the GDPR themselves, as they do not exercise any control over personal data of users, but simply provide a platform for app providers to offer their apps.[61] However, app stores can impact on the manner in which third-party apps – who do qualify as data processors – handle data protection.[62] Moreover, they are encouraged by the GDPR to fulfil this role.[63] In this regard, app stores conduct a form of industry self-regulation.[64] While app stores voluntarily impose these rules on third-party apps, although encouraged by the GDPR, self-regulation is not voluntary from the point of view of the app developers. In order to examine these app stores' behaviour towards privacy of mHealth apps and to assess the effectiveness of these existing practices for health data protection in mHealth apps, this paper performs a case study analysis on Apple App Store and Google Play, today's leading app stores.[65]

4.3 Case Studies

4.3.1 Apple App Store

In order for app developers to submit apps to the Apple App Store, they must register to the Apple Developer Program, governed by the Apple Developer Program License Agreement.[66] Furthermore, Apple App Store reviews all submitted apps and app updates according to the App Store Review Guidelines.[67] As shown in table 1 above, these Guidelines contain specific rules on mHealth apps and state that these apps may be reviewed with greater scrutiny.[68] The guidelines also contain general

[58] Apple.com, *supra* note 12; Google Play, *supra* note 12.
[59] Fong, *supra* note 13, 96-98; Hestres, *supra* note 13, 1265-1280.
[60] THE NETHERLANDS AUTHORITY FOR CONSUMERS & MARKETS, *Market study into mobile app stores* 40 (2019).
[61] EUROPEAN UNION AGENCY FOR CYBERSECURITY, *supra* note 68.
[62] *Id.*
[63] Recital 78 GDPR.
[64] Fong, *supra* note 13.
[65] App Stores List (2019), BUSINESS OF APPS (2017), https://www.businessofapps.com/guide/app-stores-list/ (last visited Feb 24, 2020).
[66] Apple Developer Program License Agreement 2020.
[67] Apple.com, *supra* note 12.
[68] *Id,* §1.4.1.

provisions on processing of personal data and privacy. First, apps must include a privacy policy, explaining how users can exercise their rights to data retention, deletion and withdraw consent.[69] Second, data collection must be based on user consent and users must be provided with an easily accessible and understandable option to withdraw consent.[70] Third, apps should minimise data collection.[71] With regard to sharing of data with third parties, user consent is required.[72] Furthermore, apps should not attempt to build a user profile on the basis of collected data.[73] The Apple Developer Program License Agreement also states that app developers must take into account user privacy and comply with privacy legislation.[74]

Furthermore, as can be seen in table 1, the guidelines contain explicit rules on *health* data processed by mHealth apps.[75] First, apps may not use or disclose collected health data to third parties for the purpose of advertising, marketing or other data mining purposes.[76] In addition, apps may not use health data for targeted or behavioural advertising.[77] However, they may use or disclose health data for purposes of improving health management and health research, but only with user permission.[78] Second, app developers may not write inaccurate data into mHealth apps.[79] Third, mHealth apps may not store health information in iCloud.[80]

4.3.2 Google Play

Google Play's review criteria are outlined in the Developer Distribution Agreement and Developer Program Policies.[81] The Agreement functions as legally binding contract between the app developer and Google.[82] With regard to processing of personal data, the Agreement states that apps should comply with applicable data protection laws.[83] More specifically, apps must inform users of what personal data is processed, provide a privacy notice and offer adequate data protection. Furthermore, apps may only use personal data for the purposes the user has consented to.[84] As shown in table 1 above, the Agreement does not specifically mention mHealth apps or health data.

---

[69] App Store Review Guidelines 12 September 2019, §5.1.1 (i).
[70] *Id*, §5.1.1 (ii).
[71] *Id*, §5.1.1 (iii).
[72] *Id*, §5.1.2 (i) and (ii).
[73] *Id*, §5.1.2 (iii).
[74] Apple Developer Program License Agreement 2020, §3.3.7- 3.3.11.
[75] App Store Review Guidelines 12 September 2019, §5.1.3.
[76] *Id*, §5.1.3 (i).
[77] *Id*, §3.1.7.
[78] *Id*, §5.1.3 (i).
[79] *Id*, §5.1.3 (ii).
[80] *Id*.
[81] Google Play Developer Distribution Agreement 5 November 2019.
[82] *Id*, §2.1.
[83] *Id*, §4.6.
[84] *Id*, §4.8.

The Developer Program Policies provide more guidance on processing of personal (health) data. With regard to processing of personal data, the Policies state that apps that are intended to abuse or misuse personal data are strictly prohibited.[85] Furthermore, apps must be transparent about the collection, use and sharing of personal data.[86] As to sensitive personal data, which probably also include health data, the Policies state that collection and use should be limited to purposes directly related to functionality of the app. Furthermore, an accessible privacy policy must be posted within the app itself. It must also disclose the type of parties the sensitive data is shared with.[87] Moreover, the in-app disclosure must contain a request for users' consent prior to data processing, requiring affirmative user action. These permission requests must clearly state the purposes for data processing or transfers. Furthermore, personal data may only be used for purposes that the user has consented to.[88] The Policies do not contain explicit provisions on mHealth apps, except for a prohibition on false or misleading health claims.[89]

4.3.3 Case Study Analysis

The above examination of app stores' guidelines shows that app stores are indeed concerned with privacy issues. However, it is questionable whether this leads to a higher level of protection of mHealth

Table 1 Health Data Protection in App Store Policies

	Apple App Store	Google Play
Operating system	iOS (e.g. iPhone)	Android (e.g. Samsung Galaxy)
Amount of apps	+- 2.2 million apps	+- 2.6 million apps
Pre-approval procedure	✓	✓
Deletion of non-compliant apps	✓	✓
Requirement to comply with privacy legislation	✓	✓
Requirement to integrate privacy policy	✓	✓
Explicit inclusion of the GDPR data protection principles	✓	✗
Explicit inclusion of data subjects' rights	✓	✗
Explicit rules on user consent	✓	✓
Rules on mHealth apps	✓	✗
Rules on health data	✓	✗
Requirement of explicit consent for health data processing	✗	✗

Source: author's analysis (2020)

app users' health privacy. Both app stores' guidelines state that apps must comply with privacy

[85] Google Play Developer Program Policies, under 'Privacy, security and deception'.
[86] *Id*.
[87] *Id*.
[88] *Id*.
[89] *Id*, under 'Unapproved Substances'.

legislation and integrate a privacy policy. However, the level of detail of the respective app stores' privacy provisions differs significantly. While Apple App Store specifically recalls most of the GDPR's data protection principles and data subjects' rights, Google Play's privacy guidelines are formulated in somewhat vague terms and do not mention data subjects' rights. Therefore, Google Play's guidelines do not offer app developers the needed guidance on *how* to protect personal data, specifically with regard to data subjects' rights. This entails a strong risk that users' rights will simply end up in the app's privacy policy fine print and will not lead to better privacy protection in practice.

Furthermore, while Apple App Store has specific guidelines on health data processing, Google Play's Policies only mention "sensitive personal data". This lack of specific regulation of health data does not reflect the risky nature of this type of data and therefore does not increase awareness of the need for protection. Most notably, both guidelines miss a provision on "explicit consent" for health data processing, which is required for app developers under the GDPR. While both guidelines contain provisions on user consent, no distinction is made between "regular" and "explicit" consent and thus no clarification on how to obtain explicit consent is offered. This puts privacy at risk, as control over health data is not sufficiently protected.

Both guidelines state that non-compliant apps will be removed, but do not elaborate on the structure of the monitoring process. Therefore, actual enforcement of the guidelines faces risks of uncertainty and inconsistency, which does not ensure compliance with the GDPR. After all, app stores are likely facing the same capacity problems as data protection authorities and it could take months before non-compliant apps are taken down. Compliance issues also come into play in the differences between the respective guidelines, as this leads to the risk of unequal standards of protection of iOS and Android users.

Taken together, it can be concluded that the current self-regulation practices, Google Play's especially, do not live up to their potential and do not adequality ensure mHealth app users' control over their health data. However, due to the central position of app stores, self-regulation by app stores may still contribute to a higher level of health data protection if certain amendments are made to the content and form of their policies. Recommendations on how to improve the policies are touched upon in the next section.[90]

5. Recommendations to Improve Current App Store Self-Regulation Practices

App stores have a powerful position in the mHealth app sector. By setting requirements for mHealth apps to be listed on and removed from their platforms they hold the most promising means to improve the level of health data protection of users. Their current self-regulation practices could be improved on multiple fronts. First, app stores could provide app developers with clearer guidelines on data processing obligations and data subjects' rights. This should include stating all applicable obligations and rights

[90] This section does not consider intermediary liability under the e-Commerce Directive.

under the GDPR and providing practical guidance on how to adequately implement this in apps. For example, apps stores could issue technical guidelines on how to include consent withdrawal mechanisms in the apps. Translating privacy rights to technical measures will enhance adequate understanding and implementation by app developers.[91] Furthermore, app stores could make data subject rights and principles part of their contractual agreements with app developers to further strengthen compliance.[92]

Second, specific provisions on health data protection should be included, in order to point out its importance and increased privacy risks. These provisions should at least include the requirement to obtain explicit consent on health data processing and provide technical guidance on how to implement this.[93] There should also be specific provisions on limiting sharing of health data with third parties and possible commercial use. Additionally, app stores can further strengthen users' control by requiring apps to include user report tools on data protection infringement or provide for these tools in the app store itself.[94] Furthermore, app stores should commit to raising awareness on the risks of health data processing. For instance, a standard text on the risks could be provided for in the guidelines, which app developers would be required to include in their privacy policies. App stores could educate users of the risks by adding 'health data processing warnings' to the downloading environment.

Moreover, app stores could strengthen user protection if they would mainstream their policies and engage in a shared EU Code of Conduct under the GDPR.[95] GDPR codes are voluntary tools which set out specific data protection rules. They provide a detailed rulebook for controllers and processors in a specific sector. Bodies representing a sector – such as app stores – can create codes to aid GDPR compliance.[96] Codes have to be approved by the European Data Protection Board (EDPB) and compliance will be monitored by an accredited, independent supervisor.[97] Consequently, present self-regulation would turn into co-regulation and current guidelines would be replaced or supplemented by this GDPR code. App stores could make adherence to the code by app developers a requirement to offer apps on their platforms. This would have more effects than current self-regulation initiatives as pre-approval of the code by the EDPB will give the code greater authority and the monitoring mechanism will lead to better compliance. Moreover, the unequal level of protection and risks of legal uncertainty and inconsistency would be minimised.[98] For mHealth app users' health privacy, a GDPR code will provide for more transparency regarding apps' approaches to data processing.[99] For example, the code

---

[91] ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 58.
[92] Fong, *supra* note 13, 108-111.
[93] Bashir et al., *supra* note 27.
[94] Daithi Mac Sithigh, *App law within: rights and regulation in the smartphone age*, INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 154–186 (2013).
[95] Art. 40 GDPR.
[96] EUROPEAN DATA PROTECTION BOARD, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (2019) 6.
[97] *Id.* 8; Art. 40(5), 40(9) and 41(1) GDPR.
[98] Maximilian von Grafenstein, *Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design*, *in* RESEARCH HANDBOOK ON PRIVACY AND DATA PROTECTION LAW: VALUES, NORMS AND GLOBAL POLITICS (Forthcoming).
[99] EUROPEAN DATA PROTECTION BOARD, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (2019).7-9.

would have to include specification of all applicable rights related to control over health data, explicit consent included.[100]

The preceding sections allow for the conclusion that app stores could positively impact GDPR compliance and thus strengthen mHealth users' health privacy by engaging in a GDPR code with specific health data safeguards. While there is no guarantee that app stores will make these changes, there are compelling reasons for them to do so. Foremost, the increased legal certainty offers app stores a competitive advantage. It reduces the complexity of app developers' entrepreneurial process which may positively impact app stores' businesses.[101] For app developers, a code would be beneficial because it could be used to demonstrate compliance with the GDPR.[102] Furthermore, app stores will benefit from good privacy practices by third-party apps because this will likely also enhance their own trustworthiness. In this regard, privacy can be seen as a positive marketing statement.[103] Moreover, both Apple and Google were stakeholders in the European Commission's attempt on a voluntary mHealth Privacy Code of Conduct, which shows their interest in such an initiative.

6. Conclusion: Improved App Store Self-Regulation Strengthens Health Privacy

Paradoxically, the wish to achieve self-empowerment by using mHealth apps leads to users surrendering power due to a lack of control over their health data. While the GDPR offers a solid solution for the protection of mHealth app users' health data in theory, it lacks practical effectiveness. Self-regulation of third-party apps by app stores by means of review procedures could fill the regulatory gap and thereby contribute to the level of health data protection in the EU. However, the performed case studies show that current self-regulation does not fulfil this promise. Nonetheless, given the platforms' central and powerful position in the sector, complementary regulation of mHealth apps by app stores may still be the most promising means to improve the level of health data protection of mHealth app users. This conclusion sheds light on the heavily debated role of the EU in regulating technological phenomena and related fundamental rights risks: in some cases, the sector itself is in a better position to regulate these risks and enforce legal compliance than independent supervisory authorities. This finding is in line with the EU's growing tendency to promote and support self-regulation structures to supplement EU legislation.

Despite the important role of app stores in achieving this, in the end, the ultimate responsibility for safeguarding users' health privacy lays with the mHealth app developers and providers that process health data. mHealth apps should provide users with the adequate means to exercise privacy rights by ensuring concrete and effective opportunities to have control over decisions regarding health data processing. In this regard, effective possibilities for actual enforcement of self-regulation standards are

---

[100] Art. 40(2) GDPR.
[101] von Grafenstein, *supra* note 123.
[102] See §3.2.3; Art. 24(3) GDPR; EUROPEAN DATA PROTECTION BOARD, *supra* note 112, 9.
[103] Mulder, *supra* note 6.

of key importance. While app store self-regulation may steer mHealth app developers in the right direction by translating the GDPR's privacy provisions into technical pre-approval requirements, compliance with the relevant privacy provisions is also aided by increased awareness among both mHealth users, developers and health data brokers as to the risks mHealth apps entail for individual fundamental rights. The EU could play a central role in accomplishing this, in order to assist mHealth users to achieve the highly desired self-empowerment by bringing the GDPR to life in mHealth apps.