UiO : Faculty of Law
University of Oslo

Mobile health apps

The enforcement of proposed consumer remedies and their influence on data protection law

Candidate number: 7017

Submission deadline: 01.12.2018

Number of words: 15.233

Acknowledgements

By completing this paper, I close one paramount chapter of my life. With this, I planted the seeds of knowledge which will slowly grow into a ferocious, brave tree. I am looking back now realizing how much every professor and mentor contributed to this growth process. For this, I would like to express my gratitude for their lessons, be they of law or of life. And, as trees cannot grow without the touch of the gentle and smiling sun, I want to thank my parents and dear ones for their continuous care and concern.

I am confident that, one day, this tree will add to the oxygen so necessary for human existence.

Table of contents

Abbreviations

DCD	Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content
GDPR	General Data Protection Regulation
DP	Data Protection
WP29	Article 29 Working Party
RTDP	Right to data portability
CRD	Consumer Rights Directive
MHA	Mobile Health Applications

1 Introduction

The basis of growth in our society has been the exchange of goods.[1] In the beginning, a family was self-reliant and growing everything within the vicinity of their yard. Nowadays, in our capacity as consumers, we are at a click distance from buying online (almost) every product we wish,[2] from clothes to smart facial mask treatments.[3] In order to do that, we need to provide to the supplier personal information about ourselves such as name, address, or payment details. In this situation, we are both consumers and data subjects at the same time. In light of our need and demand to consume content online, the market adjusted, and it offers us content for which we, allegedly, no longer need to pay a price, be it in Euro or Bitcoins. The European legislators did not turn a blind eye to these changes and have been working hard towards fulfilling the goals designed under the Digital Single Market policy.[4] One of the topics which evolved organically as driven by the market[5] concerns the interplay between data protection and consumer law, specifically the subject of consumers *buying* digital content in exchange of their personal data. The option chosen by the European Commission (**the Commission**) to define this new type of transaction refers to digital services which are supplied not in exchange for a price but against counter-performance other than money.[6]

In essence, the Commission wants to empower consumers by conferring them the same rights as when they buy a product for a price.[7] In the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (**DCD; the Proposal**) a thought-provoking set of rules has been proposed in relation to the purchase of digital content.

[1] History world, "History of trade", <http://www.historyworld.net/wrldhis/PlainTextHistories.asp?historyid=ab72>, accessed 10 November 2018.

[2] Excluding unlawful and dubious dealings on the darknet.

[3] CNET, Weirdest products at CES <https://www.cnet.com/pictures/ces-2018-weirdest-gadgets/> accessed 10 November 2018.

[4] European Commission, A Digital Single Market Strategy for Europe, May 2015: "The Digital Single Market is a strategy of the European Commission to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection" and it is built on three pillars: "better access for consumers and businesses to online goods and services across Europe, creating the right conditions for digital networks and services to flourish and maximising the growth potential of our European Digital Economy.", <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN> , accessed 10 November 2018.

[5] As scholar Frederik Z. Borgesius emphasized in a workshop: "Consumer law and data protection do interact in a reality, where the market is hovering up data.", answering to the question whether consumer protection should intertwine with data protection law, "The relationship between EU consumer law and data protection", <https://brusselsprivacyhub.eu/publications/ws13.html>, accessed 10 November 2018.

[6] Recital 13 DCD.

[7] Ibid.

The DCD is the result of the rejecting the former proposal of the Commission on the Common European Sales Law because it did not "fully unleash the potential of e-commerce in the digital market".[8] The main novelty in the DCD is referred to in Article 3(1), which widens the scope to digital content supplied to the consumer when the consumer actively provides counter-performance other than money in the form of personal data or any other data. Basically, this means that the consumer should benefit from the same level of protection as to the digital content paid for a price. The DCD refers to three sets of rules:[9] rules on conformity of the digital content, remedies available to consumers and certain modalities for exercising these remedies. As of March 2018, the European Parliament (EP) has been working on the first reading position and proposed a new legislative resolution.[10] The next step involves first reading by the Council, followed by a second reading by the Parliament. Additionally, the DCD is a top priority in 2018[11] for the three EU law-making institutions.[12] The most recent Briefing produced by the European Parliament on the DCD[13] specifies that an ongoing issue concerns the relationship between the Proposal and EU public-law rules on the protection of personal data.

Privacy and data protection have been considered one of the legal hypes for the past two years. Even if it is a relatively recent legal field,[14] it becomes more and more pervasive into other areas of law. For the purposes of this paper, we will observe how a public legal instrument (GDPR) and a private piece of legislation from a different area of law exert influence on each other and sometimes lead to contradictory results. Moreover, it is important to bear in mind that due to its public law nature seeking to protect the fundamental rights of individuals,[15] GDPR rules will always prevail despite of any contractual provisions between parties.

[8] Annex II (withdrawn initiatives) 2015.

[9] Recital 8 DCD.

[10] EP, 'Report on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0375&language=EN> accessed 11 November 2018.

[11] Joint Declaration 2018, <http://www.europarl.europa.eu/oeil/popups/thematicnote.do?id=2063000&l=en> accessed 11 November 2018.

[12] European Parliament, the Council and the European Commission, Articles 14, 16, 17 Treaty of the European Union.

[13] European Parliament, Briefing – EU legislation in progress, Contracts for the supply of digital content and digital services, February 2018.

[14] Lee Bygrave, 'Data Privacy Law: An International Perspective', Oxford University Press, 2014, 13.

[15] Article (1) GDPR.

In data protection law, there are two important roles which must be determined before the start of any processing operation: controller and processor.[16] The controller determines the means and purposes of the processing whereas the processor processes data on behalf of the controller. Even if the processor has a more limited role, a number of specific obligations must be complied with.[17] In the relationship with data subjects, the controller plays a direct role: he should inform the individual about the processing and respond to requests. For this reason, I am not considering the role per se that the supplier has in the processing since the discussion is focused on the data subject/consumer.

1.1 Research and problem questions

The general question that this paper aims to answer is:

> *How is the relationship between consumer protection law and data protection law harmonized in the EU digital market in the context of mobile health applications?*

As a point of departure, sets of actual and proposed rules are used to understand and problematize the relationship between consumer protection and data protection as applied for mobile health applications. To be able to address the research question comprehensively, the following factors are taken into consideration:

1. Added value for consumer protection in comparison with the current rights under the data protection framework;
2. (Lack of) awareness of consumers about data protection and consumer rights in a digital context;
3. Scarcity of consumer actions against mobile health app developers.

Since the scope of DCD is very wide, I opted to analyze one specific type of digital services, those provided by developers of mobile medical health apps (MHA). This case study emerged because MHAs refers to a commercial product that involves the collection of high amounts of data which, observed in context, most likely fall under the category of special and sensitive categories of data. Moreover, their ubiquity in the Western society makes them highly relevant as they are usually offered for free or for a small pay considering the significant effects for the user's health because of following MHAs. Finally, this example entails a mix of consumers/patients that usually just uninstalls the app without further remediation action.[18]

[16] Article 4(7) and (8) GDPR.

[17] Article 28 GDPR – Processor. On top of that, processors of personal data must comply with general data protection obligations (e.g. principles, lawful bases).

[18] <https://ag.ny.gov/press-release/ag-schneiderman-announces-settlements-three-mobile-health-application-developers>. Example of a singular case in the US where action was taken against developers;

Based on these, a theoretical exercise will be carried out to ascertain to what extent remedies in DCD add value to the remedies that consumers already benefit from under current applicable data protection law.

1.2 Methodology

This paper is developed based on classic doctrinal legal research.[19] First, I analyze the law as it is (*lex lata*) which constitutes the touching points between consumer protection and data protection. Then, the aim is to fit these rules into the existent legal framework while following the legal coherence in both areas of law. On the one hand, consumer law aims to protect the consumer by ensuring fair contract terms. On the other hand, data protection scope is to protect personal data and privacy. The end goal of this paper is to contribute to shaping the law as it should be (*lex ferenda*).

1.3 Paper structure

Firstly, an overview of the relevant concepts is presented referring to digital content, personal data, provision of personal data and its value. Secondly, light will be shed on the use of mobile health apps, with an accent on their significance from a EU legal standpoint. Thirdly, the current remedies proposed by the DCD will be analyzed and compared with DP rules. Fourthly, particular attention is given to data portability in comparison with the right to receive your data back under DCD. Naturally, conclusions and matters worth of further research complete the paper.

1.4 Literature review and delimitation

Recently, the topic on the interplay between data protection and consumer law has been discussed extensively.[20] One recurring controversial question refers to whether the Commission, by conferring the same rights to consumers who receive free services in exchange of their personal data, acknowledges that personal data can be monetized. The legislator's standpoint is that, by proposing the DCD, it recognizes a certain business model based entirely on the collection of personal data.[21] Hence, otherwise different levels of consumer protection would be afforded and 'an incentive for businesses to move towards

---

<https://mhealthintelligence.com/news/consumers-doctors-still-arent-agreeing-on-mhealths-goals>. Research showing consumers do not fully understand how MHAs function.

[19] 'Doctrinal research lies at the heart of any lawyer's task because it is the research process used to identify, analyse and synthesise the content of the law.' Terry Hutchinson, Doctrinal Research: Researching the jury in Dawn Watkins and Mandy Burton (eds), Research methods in Law (2nd ed, Routledge, 2018), 13;

Paul Chynoweth, 'Legal Research'.

[20] For example, subject of a legal conference: Consumer Law in the Data Economy, Amsterdam, April 2018.

[21] Recital 13 DCD.

offering digital content against data'.[22] While this paper does not aim to provide a definite answer since that would be out of scope, it will touch upon points emphasizing that businesses do produce profit from personal data.

The starting point for this paper is the well-acclaimed article *The Perfect Match? A closer look at the relationship between EU Consumer Law and Data Protection Law* by Helberger, Borgesius and Reyna – a trio of consumer and data protection law experts. The premise of their article is that data protection and consumer protection regimes should apply in parallel, thus offering 'a sufficiently diverse toolbox of rights and remedies to provide a high level of protection of consumers in digital markets.'[23] They also refer to the legal duo as *data consumer law*.[24] Applying data consumer law rules to mobile health applications aims to discover whether the toolbox actually provides real consumer protection.

The usual perspective regarding DCD concerns the general implications of consumer law for data protection. For instance, Rott describes the role of consumer organizations in enforcing data protection rules.[25] An interesting standpoint is that of Svantesson, who describes the two sets of laws in a visual fashion: consumer law sets a floor to pursue high consumer protection whereas data protection law aims to protect individuals and ensure free movement of data.
With regards to MHAs, research on the effect of consumer protection is scarce. In general, there is an ongoing discussion about the associated security and privacy risks[26] with limited attention conferred to remedies that consumers could have against untrustworthy developers or businesses. Consequently, this paper aims to fill that gap in the applicability of consumer and data protection rules to electronic health.

[22] Ibid.

[23] Natalie Helberger et al, 'Consumer law and data protection law', 1429.

[24] Ibid, 1427.

[25] Peter Rott, 'Data protection law as consumer law – How consumer organisations can contribute to the enforcement of data protection law', EuCML, Issue 3, 2017, 113 – 119.

[26] See chapter 3.

2 Relevant norms and concepts

2.1 Personal data - as counter-performance

A concept relevant to our discussion is that of personal data and more specifically, when it is provided as counter-performance. As per GDPR,[27] personal data refers to any information relating to an identified or identifiable natural person. For example, personal data ranges from names, e-mail addresses to political opinions expressed on social media. The most important aspect concerns the context in which we discuss about personal data. While it may be possible to identify a person based on their name, date of birth and location regardless of context, in the case of a personal opinion, a name, computer id and location are conducive to identifying the natural person.

The novelty brought by DCD in regarding personal data as counter-performance[28] is seen as a confirmation of an approved social practice[29] according to which consumers pay with their personal data for free services. A recent research study[30] shows that individuals who are more likely to disclose personal data are the ones who prefer to have greater control over information flows.[31] Furthermore, a caveat is that their willingness depends on the type of personal data that will be shared: they are more prone to share data concerning their online persona than information on their physical identity and financial records.[32] This could have implications on the remedies proposed in DCD. If the final version of the remedies passes the test of time, it would be interesting to study whether there is any influence of the type of data which has been provided on the exercise of consumer remedies by users.
Furthermore, as underlined in the Impact Assessment, the introduction of the same protection standards for 'free' digital content will increase consumers' awareness of the economic value of their data.[33] It is commonly expected that the higher the price for a product, the higher the quality expectations concerning the content provided.[34] In return, consumers would gradually expect the same quality from both types of services.

[27] Article 4(1) : 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[28] Article 3(1) DCD.

[29] Metzger, 8.

[30] Christine Prince, 'Do consumers want to control their personal data? Empirical evidence', International Journal of Human-Computer Studies, Volume 10, February 2018, 27.

[31] Ibid, 29.

[32] Ibid, 30.

[33] Commission Staff Working Document, 'Impact Assessment'.

[34] Marco Loos and Chantal Mak, 'Remedies for buyers in case of contracts or the supply of digital content', 180.

There has been an increasingly high academic debate on the value of personal data for the past years,[35] but the EU legislators have not taken any concrete steps in this direction. Instead of following the trend indicated by most academic and business, the EU Commission opted for not recognizing that data has a price. The main argument of the Commission and its supporters is that data should not be treated as a common commodity.

That being so, the Proposal takes into account, *inter alia*, whether the digital content is supplied in exchange for a price or counter-performance other than money.[36] This seems to indicate that digital content has distinct economic values based on the method of payment, i.e. money or personal data. This is contradiction with the aim of the Commission for the DCD. While taking into account that the legal instrument is a directive[37] and Member States can further specify what this criterion entails, there is a high risk of misinterpretation. Conversely, Malgieri and Custers argue that it is not impossible to assign a monetary value to personal data if the following are described precisely: expression of the monetary value, which object is being priced and how to attach value to the object. Especially the last element is subjective. A concept such as a defined reasonable value[38] can be a solution provided that a European standard is ensured.

The DCD implies that consent is the only applicable legal basis. In short, if consumers have their data processed based on other legal bases in Article 6 GDPR, remedies under DCD do not apply.

All the above show that, as Wendehorst claims,[39] implications for treating the data as "counter-performance" are not completely analyzed.

2.1.1 Variations of the 'free price' definition

In light of this, the General Approach of the Council leaves less room for ambiguity by clarifying the scope and referring to services for which consumers pay with money and for which they pay with data.[40] An innovative point is the addition of price as a digital

[35] Godel et al, 'The Value of Personal Information: Evidence from Empirical Economic studies'. In this paper, authors look at papers written 10 years before where data was already perceived as having a price. Recently, there is an abundance of papers on this topic (see SSRN for example).

[36] Article 6(2)(a) DCD.

[37] Hence not directly applicable in the legal system of the Member States. <https://ec.europa.eu/info/law/law-making-process/types-eu-law_en>, accessed 10 November 2018.

[38] The assessment for *reasonable value* could be performed based on the people's expectations on the level of improvement brought by the MHA in their lives.

[39] Christiane Wendehorst, <The Proposed Digital Content Directive and its Implications for the Data Economy>, slide 11.

[40] Article 3(1) General Approach.

representation of value including virtual currency[41] which acknowledges the current hype and increasing recognition of this type of payment. As expected, the Council specifies that virtual currency seen as payment only applies to the extent that Member States recognize them.

The European Parliament refers to supplying a digital service "to the consumer through the payment of a price or under the condition that the data is provided by the consumer or collected by the trader or a third party in the interest of the trader."[42] The wording "in the interest of the trader" refers to access to the service under the condition of receiving a service in exchange of the use of data by the supplier which might still cause tensions with Article 7(4) GDPR.[43] Accordingly, consent would not be freely given in this case as the processing would be carried out on this legal basis while consent is not necessary for such performance.

Unfortunately, this change by the EP is prone to create even more confusion for suppliers. Whereas the DCD rules apply without prejudice to GDPR,[44] the change proposed by the EP leads to an overarching DCD.

2.1.2 Digital content

In order to understand how remedies could be exercised in practice, it is important to consider what type of digital content they cover. Firstly, the DCD defines digital content as data or services in Article 1:

'digital content' means:

> (a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software,
> (b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and
> (c) a service allowing sharing of and any other interaction with data in digital form provided by other users of the service.

Additionally, Recital 19 mentions that a service which is delivered through a digital environment does not represent digital content as such (i.e. translation services by a human translator). In this paper, terms 'digital content' and 'content' are used interchangeably if not mentioned otherwise. For instance, an app measuring your sports activity provides you with

[41] Article 2(6) General Approach.

[42] Parliament Report, Article 3(1).

[43] Robert, Smit, 'The proposal for a directive on digital content', 16.

[44] Or as more clearly specified in the Council General Approach: Union law on the protection of personal data applies to any personal data processed in connection with contracts [...]. General Approach, 13.

videos on certain physical exercises based on your fitness level.[45] This is considered a 'free service' in the sense that the consumer does not pay a price for it.[46] Consequently, it seems that the DCD would be applicable to all services. However, this is not the case[47] as the DCD mentions that the consumer must provide the data actively[48] to the provider. From the perspective of the origin of data, four types can be described:[49]

- provided refers to data given by individuals consciously (e.g. social network postings, by filling in a survey);
- observed data is recorded automatically (e.g. cookies, sensor technologies);
- derived data is extracted from other data in a simple manner (e.g. calculating credit ratios);
- inferred data is produced by using complex analytics-related technologies (e.g. profiling to determine credit risk type).[50]

Firstly, the fact that the DCD only refers to provided data has further influence on the set of remedies that consumers can rely on. Secondly, the specification "actively" renders the Proposal inapplicable where suppliers process personal data of consumers without the latter performing affirmative actions.[51] Due to heated debates concerning the dichotomy between the new terminology and that used in the data protection realm,[52] this term has been erased in the proposals of the European Parliament and European Council.[53]

The choice of conferring the same rights to consumers that acquire digital content by paying a price or providing data as counter-performance does not only have an impact on consumers as such but also on businesses. In the words of the Commission, not regulating the "transaction" against personal data would "discriminate between different business models and would provide an unjustified incentive for the businesses to move towards offering digital content against data".[54] While this approach takes a fair competition law and consumer law

[45] Freeletics app, <https://www.freeletics.com/en>, accessed 10 November 2018.

[46] However, "nothing in the digital world is free". See recent scandal on Facebook and Cambridge Analytica. Scott, "Politicians follow in Facebook's footsteps on mass data collection."

[47] EDPS 'Opinion 4/2017', para 38.

[48] Recital 14, Art. 3(1) DCD.

[49] Martin Abrams, "The origins of Personal Data and its Implications for Governance", The Information Accountability Foundation, <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf> accessed 11 November 2018, 6 – 11.

[50] ICO, Big data, Artificial Intelligence, machine learning and data protection, 13.

[51] EDPS, (n47), para 41.

[52] GDPR makes no distinction between data actively or passively provided.

[53] European Parliament, Report on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content: Recital 14, Article 3(1); Council of the European Union, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (First reading) - General approach, 4.

[54] Impact Assessment, 123.

perspective, the details relevant to the implementation remain to be polished. As the devil is in the details, the justification for offering similar protection is welcomed; however, assessments of non-conformity in light of content received in exchange of personal data are still in an incipient phase.

3 Mobile health applications

Part and parcel of being a digital persona means solving our health problems by using different technologies in an area commonly referred to as digital health or e-health.[55] One type of such technology concerns mobile applications dedicated to helping us with clearing our mental and physical pains. These products have been on the rise for the past years, and more recently, they became interconnected with attached devices such as smart watches, weight scales or other sorts of measurement tools.

3.1 Definition and classification

A mobile app refers to a type of application software with a limited function designed to run on a mobile device.[56] More specifically, mobile health apps (MHAs) are health-related apps that aim to improve patients' lives through different designs and functionalities.[57] In this paper, 'patient' and 'consumer' terms are used interchangeably. Nonetheless, if regarded from a stricter perspective, 'consumer' refers to a weak party involved in economic transactions[58] whereas 'patient' describes 'a person receiving or registered to receive medical treatment'.[59] Since a patient is not necessarily a consumer, for the context of MHAs, it is more appropriate to refer to users as consumers.

As of January 2018, there are approximately 318,500 apps[60] available in the most well-known apps stores such as Android Play Store and iOS App Store. Furthermore, MHAs that are aimed to be used together with a measuring device (e.g. glucose level sent wirelessly to the mobile phone) are also considered medical devices.[61] Despite the very high number of apps, less than a quarter of total are in wide use.[62] Some of the most used apps are MyFitnessPal, Runtastic Running & Fitness Tracker and Fitbit[63] but these do not include apps used by patients together with healthcare providers.

---

[55] Rishi Duggal et al, Digital healthcare, 1.

[56] Techopedia, Definition mobile application, <https://www.techopedia.com/definition/2953/mobile-application-mobile-app>, accessed 11 November 2018.

[57] Cheng-Kai Kao, David M. Liebovitz, Consumer Mobile Health Apps: Current State, Barriers, and Future Directions, Clinical Informatics in Physiatry, Volume 9, Issue 5, May 2017, 1.

[58] Agnieszka Jabłonowska et al, Consumer Law and Artificial Intelligence challenges, 9.

[59] Oxford dictionary, <https://en.oxforddictionaries.com/definition/patient

[60] Intersog, The state of mobile health apps in 2018, <https://ehealth.intersog.com/blog/the-state-of-mobile-health-apps-in-2018> accessed 11 Novermber 2018. The number of apps is not fluctuating very much during one year as most of the new apps are short-lived.

[61] KNMG, Medical App Checker, 4.

[62] Dehling et al, 'Exploring the Far Side of Mobile Health', 16.

[63] Joe Hindy, '10 best health apps for Android', <https://www.androidauthority.com/best-health-apps-for-android-668268/>.

There are different classifications based on the purpose of the app, offering more detailed views but in general, consumer mHealth apps are categorized as follows:

- Wellness management: keeping track of diet, exercises, manage sleep, etc.;
- Disease management: keeping track of developments for diseases such as diabetes or asthma;
- Self-diagnosis: checks basic symptoms and suggests a health issue;
- Medication reminder: functions as a digital pillbox reminder;
- Electronic patient portal: ensures good communication between patients and provider and might also store personal medical records;
- Physical medicine and rehabilitation: provides physical exercises to patients as prescribed by physicians.[64]

Another classification has been conducted from an ethical perspective which is built on the premise that technological advancement shall not prejudice ethics and fairness:[65]

- Apps with indirect health implications such as pharmaceutical catalogues, search engines for medical articles;[66]
- Apps with direct health implication such as diagnostic finders, decision support, calculation of dosage;[67]
- Apps used for patient monitoring which mostly include apps that are connected to other medical devices.[68]

MHAs can be classified according to many standards. However, the difficulty lies in defining a MHA in the first place. Firstly, there is the app itself that the patient installs on her phone. Except for purely informative apps that do not necessarily use personal data, MHAs provide digital content in exchange of personal data. Secondly, the app per se can receive information about health from a sensor. Arguably, the raw data collected by the sensors and isolated within the medical device is not personal data[69] because no meaning can be derived about that person's health. Concurrently, if the measurements performed by the sensor are combined with other data in the MHA, that leads to a conclusion about the state of health and falls under the scope of personal data. As explained below, the current state of EU data protection regulation of mobile health apps does not look at the level of impact on the user's health but at the type of data that is processed.

[64] Kao, Consumer Mobile Health Apps, 3.

[65] Mary Sharp, Declan O'Sullivan, 'Mobile Medical Apps and mHealth Devices: A Framework to Build Medical Apps and mHealth Devices in an Ethical Manner to Promote Safer Use – A Literature Review, Informatics for Health: Connected Citizen-Led Wellness and Population Health', 2017, 364.

[66] These apps are out of the scope of this paper since they do not bear significant relevance for the collection of personal data.

[67] Idem (n49).

[68] Ibid.

[69] WP29, Annex – health data in apps and devices, 3.

A relevant point refers to the sources of revenue for MHA developers. These methods are specific to mobile apps in general and only some particularities are specific to MHAs. There are six established revenue models.[70] The least desired by users constitutes the free and containing advertisements model followed by freemium. The latter offers to the user basic content but in order to benefit from other services she has to pay a certain fee.[71] Similarities can be observed with the in-app purchases as source of revenue where users pay only for the functionalities that they want to access. The next model refers to the paid version of an app, which can be a one time pay or describing the fourth model, by subscribing. The advantage of a subscription for developers is that it constantly reminds users to pay. On top of that, the sponsorship model[72] describes a collaboration between the app developer and another company selling different products but that has approximately the same target group. Last but not least, a distinctive model for the MHAs is the selling of aggregated personal data to health researchers and institutions or even fitness experts, pharmaceutical companies and life insurance businesses.[73]

3.2 Data processing regimes (EU and US)

In general, the regulation of mobile health apps constitutes a fuzzy area in both the EU and US. On the one hand, the US follows a hands-off approach where MHAs encouraging a healthy lifestyle are left out of the scope of the regulation.[74] The Food and Drugs Administration (FDA) is trying to minimize the verification of pre-release on the market of as many low-risk technologies as possible.[75] This approach is understandable for certain apps which are not very invasive simply considering their impact on health is limited and the technology advances at a higher speed than the regulation.

On the other hand, as briefly hinted, the EU regulation of eHealth is highly non-uniform.[76] The only European document specific to MHAs is the EU Commission Green Paper on

[70] Morgan, How to monetize mobile healthcare apps, <https://www.healthworkscollective.com/monetize-mobile-healthcare-apps/> accessed 11 November 2018.

[71] Think Mobiles, How do free apps make money on Android and iOS in 2018. <https://thinkmobiles.com/blog/how-do-free-apps-make-money/>; Sonders, A bunch of average app revenue data… and why you should ignore it. <https://medium.com/@sm_app_intel/a-bunch-of-average-app-revenue-data-and-why-you-should-ignore-it-2bea283d37fc>; Dr. Hemper Digital Health Network, Who is really making money in the digital health apps market?; <https://www.dr-hempel-network.com/growth-of-digital-health-market/global-digital-health-apps-market/> , all accessed 11 November 2018.

[72] Ibid

[73] Idem (n64).

[74] Druggal, 1.

[75] Ibid.

[76] Chiara Crico et al, 'mHealth and telemedicine apps: in search of a common regulation', Special Issue, Journal of Cancer, 3.

mobile Health[77] and the proposed draft Code of Conduct,[78] which has been further criticized by the WP29 for not being clear enough.[79] On the other hand, the EU has introduced a Medical Device Framework with the Maastricht Treaty of 1992.[80] Accordingly, all medical devices must fulfill a set of requirements as defined in the Annex of the Medical Devices Directive. The European approach is also based on the impact that MHAs have on users.[81] On the most low-impact side of the scale, there are MHAs which do not process personal data at all. It is arguable that this is possible, but it depends on the context. For example, the number of steps a person makes for one day is not relevant if the location and walking trail are not collected. The highest-impact MHAs are connected to other sensory external devices and collect data through the app.

Having this in mind, we focus only on the data protection and consumer law perspectives, with the caveat of not following per se definition EU of medical devices that comprise MHAs.

Considering the context of the processing, MHAs most likely process sensitive data. Generally, according to Article 9(2)(a) GDPR, processing of this type of data is carried out based on explicit consent of the user. A difference should be made between the data concerning health and other types of data. For instance, the app collects user account details (i.e. password, e-mail, username) and app usage metrics. Accordingly, when asking for consent, purposes shall be differentiated for the user to make a truly informed decision. Except for the consent pop-up, data controllers must also provide certain information as per Article 13 GDPR which usually occurs in a privacy notice. Requirements for the privacy notices have been laid down in law[82] and discussed extensively by data protection authorities and businesses.[83] Hence, it is worthwhile taking into account the requirement to provide meaningful information to the user about the logic behind the use of automated decision-making.

---

[77] European Commission, 'Green Paper on mobile health ("mHealth")', <https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth>.

[78] European Commission, Code of Conduct on privacy for mobile health applications.

[79] WP 29, 'Letter of the chair on mHealth', April 2017, 2.

[80] Composed of: Medical Devices Directive, Active Implantable Medical Devices Directive and the In Vitro Diagnostic Medical Devices Directive.

[81] Idem (n75).

[82] Articles 13, 14 GDPR.

[83] See the UK Information Commissioner's Office Guide for Data Protection: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>; Mozilla Privacy Policy Guidelines: <https://developer.mozilla.org/en-US/docs/Archive/Mozilla/Marketplace/Publishing/Policies_and_Guidelines/Privacy_policies>.

3.3 Common issues related to data protection

Generally, research studies show that the most significant issues encountered by MHAs concern information security and privacy.[84] Manipulation of information provided in the app (e.g. symptoms for a migraine) can lead to an incorrect outcome and lead the user towards a wrong treatment.[85] Alternatively, loss of personal data and exposure to unknown third parties can have adverse effects on users such as damage to reputation by having their data unlawfully sold or being subject to invasive marketing. Researchers have also identified an issue from the consumers' standpoint in the field of privacy – lack of knowledge about the risks associated with sharing private sensitive health information online.[86]

Taking this into account, a marginal role of the DCD, as the Commission envisioned, is to further aid with raising awareness about the associated privacy risk of using MHAs.

3.4 Applicability of DCD

3.4.1 Scope – types of data

To begin with, we analyze the scope of DCD in light of MHAs. Article 2 DCD lays down a number of definitions. As previously mentioned, mobile apps fall under Art. 2(1)(a) which refers to digital content as data provided by applications. While the content produced by MHA is not problematic in terms of applicability, it is worth noting the relationship with the Consumer Rights Directive (CRD).

On the one hand, Art. 2(1)(a) refers to digital content as data produced and supplied in digital form (e.g. applications) and is line with the definition in the CRD.[87] However, in Recital 11 DCD, it is mentioned that this definition has a broader scope, focusing on services which allow the creation, processing or storage of data. This is clearly a reference to cloud services which are increasingly used by suppliers, including MHA developers.

If we observe *data* in an application, especially the processed data, it can include personal data. This seems to be the intention of the EU legislators since digital content can also contain personal data. While taking into account that both the scope of DCD and of CRD comprises more than personal data, we discuss the definition of processing of personal data according to Article 4(2) GDPR. Under the strict view of EU law, any operation carried out on personal data qualifies as processing. Consequently, the mention in Recital 11 DCD adds just a

[84] Dehling, 14; Dave Muoio, 'Study: Many health apps insecure, do not conform to EU privacy requirements', <https://www.mobihealthnews.com/content/study-many-health-apps-insecure-do-not-conform-eu-privacy-requirements>.

[85] Ibid.

[86] Ibid, 15.

[87] Article 2(11): "Digital content means data which are produced and supplied in digital form.", Recital 18.

clarification which could have been already inferred from CRD. Looking at the aim of the Proposal, this seems to be already hinting that it led to a duplicate legal regime for processing personal data in the EU.

On the other hand, the same recital highlights that DCD, in comparison with CRD, applies to digital content independent of the medium used for its transmission. This seems contradictory considering that Recital 19 CRD explicitly refers to tangible medium or *through any other means*. If one keeps into account that the aim of the Proposal is to broaden the rights of consumers when they receive the content for their personal data, it would be a better option to actually add valuable clarifications concerning previous Directives. Otherwise, unnecessary legal obscurity on the application of consumer and data protection regimes will flourish.

We established that MHAs fall under the definition of digital content, despite drafting shortcomings. Proving that DCD is a data-driven legislation, Article 3(1) refers to applicability in two instances: for digital content provided against counter-performance other than money, and for any other data.

For the case of an exchange between provision of services and personal data, Article 3(4) further specifies instances in which it is <u>not applicable</u>:

- Data are not further processed in a way incompatible with the following purposes and the processing is strictly necessary for:
    ii. performance of the contract or
    iii. meeting legal requirements.
- Requested data is not used for commercial purposes and it is not provided for:
    iv. ensuring the content is in conformity with the contract or
    v. meeting legal requirements.

Let's imagine the following situation: user accesses the app store on her phone, checks available apps and decides to install an MHA. An exchange of data takes places between the app store, MHA developer and user. Based on the steps in this process, we analyze how DCD applies and the influence exerted on and from GDPR.

> <u>Before downloading:</u> specific Android/iOS app store makes MHA available so that the operating system of the phone and other technical requirements are already known and checked.

The DCD does not apply because this data has the purpose to make sure the provided content is in conformity with the contract.[88] Considering that based on the context, metadata can lead to the identification of a person, it can also be regarded as personal data,[89] which leads to the application of GDPR. In addition, this is the only legal basis specific to DCD.

[88] Article 3(4) DCD.
[89] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, para 26 – 27.

For personal data, this type of processing defined under DCD falls under Article 6(1)(b) GDPR – necessary for the performance of the contract. This overlaps with the legal basis referring to the performance of the contract but it could be considered a sub-defined category of Article 6(1)(b). However, this is a caveat of DCD because it extends data protection law.

Another attention point is the addition that data should not be used for commercial purposes (i.e. for business profit). By mentioning this, drafters of DCD make clear that whatever data is technically and legally necessary to perform the contract cannot be subject to any DCD remedies. This clarification is welcome; however it still seems to be in tension with GDPR which does not differentiate between data used for commercial and not for profit purposes.

> Immediately after download: app is installed and, in general, user creates an account after she has been presented with the terms and conditions, including privacy policies.
>
> When using the MHA: the user begins generating content. For example, content can refer to the number of steps, mood, meals and the related effects on her health.

In the last two situations, personal data is collected for multiple purposes such as the creation of the account, measuring user's health or providing feedback to the developer. As per GDPR,[90] detailed information about processing of data, including legal bases for processing, is provided in the privacy policy. Accordingly, data protection law is applicable.

Interestingly, Article 3(4) DCD, by using a different wording, refers to data processing for meeting legal requirements where the supplier does not further process them in a way incompatible with this purpose. The second part of this Article refers to a well-known data protection principle: purpose limitation.[91] Firstly, there is no added value in repeating the principle here because since data protection is applicable, so are the associated principles. Secondly, DCD does not even refer to the principle in full but only to the prohibition of further processing for incompatible purposes.

Furthermore, Article 3(4) DCD refers to a processing in order to meet legal requirements, which could be read as one of the legal bases for processing in GDPR. Article 6(1)(c) GDPR describes processing for compliance with a legal obligation. While understanding that the data processed for this purpose should not fall under DCD, the dichotomy between language used in GDPR and here creates legal uncertainty.

Based on the discussion above, the data under the scope of DCD can be summarized as account specific data (including technical data) and user generated content. As explained in chapter 4.1, in the context of MHAs, sensitive personal data is processed. This operation shall

[90] Articles 13, 14 GDPR.

[91] Article 5(1)(b) GDPR: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

be based on one of the legal grounds mentioned in Article 9(2) GPDR. It is noteworthy that when the app is for free, developers usually make profits based on displayed ads.[92] Commonly, the user is targeted with ads which are generated based on the collected (sensitive) data.

[92] Think Mobiles - How do free apps make money, <https://thinkmobiles.com/blog/how-do-free-apps-make-money/>.

4 Data subjects' rights and consumer remedies in context

4.1 Data protection-specific rights

In general, data subjects' rights related to the processing of their personal data are not a legal novelty since they were already part of the old EU Data Protection Directive.[93] However, GDPR formalizes the previously implied legal obligation to give effect to the rights of data subjects in Article 12(2). Additionally, it introduces the right to erasure[94] and the right to data portability.[95]

According to Articles 13 and 14 GDPR, data subjects must receive certain information based on whether the data controller obtained their data directly or through another party – this information is found in privacy notices. Another addition to the transparency of the processing towards individuals is the right of access. The data subject must receive information on whether the processing is carried out, including details of the processing, as similarly described in the privacy notice. Furthermore, she is entitled to a copy of the data. If she observes that data is inaccurate, a request for rectification can be made.[96] During the time that the controller checks if the data is accurate, it is possible for the data subject to restrict the processing.[97] Additionally, processing can be restricted provided that it is performed unlawfully and data subjects oppose erasure, data is no longer necessary for the initial purpose but only for legal claims and during the timeframe in which the data controller reviews the legitimate basis test following the opposition by individual.[98]

The right to object to processing applies where legal bases are the necessity for the performance of a task carried out in the public interest or in the exercise of official authority and legitimate interests.[99]

In comparison with the version in the old Directive, GDPR is more specific on the right not to be subject to a decision solely on automated processing, including profiling.[100] As described by the WP29, there should be a meaningful human intervention included in the decision.[101]

By default, controllers shall respond to such requests in maximum one month from registering the request and, in more complex cases,[102] up to three months.[103]

---

[93] 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. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>.

[94] The right to be forgotten/to erasure was already part of the case-law on data protection: C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

[95] Article 20 GDPR. See in detail Chapter 5.

[96] Article 16 GDPR.

[97] Article 18 GDPR.

[98] Ibid.

[99] Article 21 GDPR.

[100] Article 22 GDPR.

[101] WP 29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 8.

[102] Controllers make this assessment based on the difficulty and number of requests received.

In terms of remedies, individuals have the right to lodge a complaint against the data controller with the supervisory authority in their country of habitual residence.[104] Moreover, any legal or natural person has the right to an effective judicial remedy against a decision taken by the supervisory authority[105] or following a complaint against the controller.[106]

4.2 Triggers for consumer remedies in DCD

After setting up the stage by explaining notions critical to understanding the background for the remedies when consumers provide personal data as counter-performance, we will explore in depth their content and applicability. Under the DCD, remedies are triggered by two causes: for the failure to supply the digital content[107] or for the lack of conformity with the clauses in the contract.[108]

4.2.1 Failure to supply the digital content

Firstly, the supply itself refers to providing the digital content to the consumer or a third party. The latter is perceived as an intermediary in the sense that it operates a physical or virtual facility and gives access to content to the consumer.[109] An example of a third party supplying content constitutes an e-mail service provider: in case of receiving an e-book on your e-mail account, access to content is conditional on the time when the e-mail server makes it available for your reading. Due to the rapid nature of the request, the content should be supplied immediately to the consumer after concluding the contract.[110] Consequently, the act of supplying takes place when the consumer receives the content or it is made available to the third party. Another example constitutes a cloud provider. Considering that the data in the MHA and the app itself are stored in the cloud, the supplier/controller is dependent on the availability of the cloud service. In this case, the cloud provider could be both a physical and virtual facility operator. However, storing data and applications with, for instance, Amazon Web Services (AWS) by using their highly reliable cloud instances leads to limited technical problems.[111] A user of MHAs will notice that the app is not functional for a couple of minutes which in the case of a health lifestyle app should not be a significant issue. It could become problematic for apps with continuous monitoring of health, such as diabetes.

---

[103] Article 12(3) GDPR.
[104] Article 77 GDPR.
[105] Article 78 GDPR.
[106] Article 79 GDPR.
[107] Article 11 DCD.
[108] Article 12 DCD.
[109] Article 5(1) DCD.
[110] Article 5(2) DCD.
[111] Status Amazon cloud, <https://status.aws.amazon.com/>, accessed 11 November 2018. Uptime of AWS severs is 100% in 99% of the time.

Recital 35 DCD clarifies that a distinction must be made between the time of the initial supply (after the contract was concluded) and the subsequent interruptions in providing the content. This distinction is of greater significance when exercising the types of remedies that are triggered by the initial lack of supply. Terms and conditions, including privacy policies, constitute the contract between user and developer. With regards to the conclusion of the contract, there are multiple possibilities: when the user downloads the app; accesses it for the first time or, most realistically, when she clicks on the infamous "Accept" button. This matter follows the Consumer Rights Directive which regulates the interaction between consumers and traders in an electronic environment.[112]

4.2.2 Lack of non-conformity with the contract

Secondly, consumer remedies will be triggered by the lack of conformity with the contract. Article 6(1)(a) DCD stipulates that the digital content shall bear the same characteristics as mentioned in the contract such as quantity, quality, duration, version, or functionality. Simultaneously, it shall be fit for the described purpose(s),[113] be updated and supplied with relevant instructions and customer assistance.[114] If the aforementioned characteristics are not described in the contract, the comparison is made between the received digital content and digital content of the same description.[115]

Other criteria relevant in assessing the quality of the digital content refers to international standards[116] or codes of conduct, and any public statements made by the supplier. Conformity is further assessed from two perspectives: based on integration into the consumer's digital environment[117] and whether the content is free of any third-party rights which would otherwise render the content unusable.[118]

Until now, we considered conformity strictly from a technical perspective. However, by the same token, the same technical requirements are enablers for data protection. Hence conformity includes respecting data protection requirements, especially principles such as data protection by design and by default. Practically, this means that apps need to be designed in such a way to differentiate between the types of data which then allows for the exercise of individuals' rights. In the case of DCD, user generated content should be extractable and

[112] Articles 6, 8 Consumer Rights Directive.
[113] Article 6(1)(b) DCD.
[114] Article 6(1)(c), (d) DCD.
[115] Article 6(2) DCD.
[116] For example, as provided by the International Organization for Standardization.
[117] Article 7 DCD.
[118] Article 8 DCD.

different from other types of data. The intertwine between the discussed areas of law shows how data protection principles are safeguarded through consumer protection law. Consequently, a violation of data protection rules is regarded as a breach of contract (e.g. information requirements) while the reverse is not necessarily applicable.

4.3 Remedies

The DCD introduces a hierarchy of remedies.[119] According to Article 12 DCD, consumers must first seek 'cure', which is a specific performance by the supplier.[120] It is worth noting that the Proposal still makes distinctions between the remedies available in case of payment for a monetary value and those aimed at helping the consumer when data was collected as counter-performance. This might already cause certain misunderstanding when applied in practice, as explained below.

4.3.1 Right to have the digital content brought into conformity

In general, if it is impossible or unlawful for the supplier to comply with the request or simply does not comply with it,[121] the consumer can seek termination, partial or total refund.[122] However, the receipt of a reduction of the price is applicable only in case of payment for a price. The supplier shall bring the content into conformity if the costs to fulfill this action are not unreasonable. In order to carry out an assessment of what constitutes reasonable costs, the following non-exhaustive criteria must be taken into account:

- The value that the digital content would have if it was in conformity from the beginning,
- If the content is not in conformity with the contract, by what percentage does it still attain its purposes? This assessment must be made by comparing digital content of the same description.

Of relevance here is the fact that the MHAs which are also considered medical devices must fulfill a series of requirements.[123] As expected, these requirements include technical, organizational, informational and ergonomic requirements.[124] This means that one way to assess the conformity of digital content is to balance its functionality against these requirements.

[119] Explanatory memorandum, pp. 12-13, Mak, The new proposal, 23.

[120] European Parliamentary Research Service, 'A legal analysis of the Commission's proposal for a new directive', 22.

[121] Article 12(1) DCD.

[122] EP, 'Contracts for supply of digital content', 22.

[123] Chapter 3.3.1.

[124] Hannah R. Marston et al, 'Mobile e-Health', Springer International Publishing AG, 2017, 256.

4.3.2 Right to terminate the contract

Article 13 DCD refers to the obligations for both parties stemming from exercising consumers' right to terminate the contract. Contracts for the supply of digital content that was not paid for with a price can be terminated in three situations, as follows. Article 11 DCD refers to a situation where content is not supplied exactly after the conclusion of the contract;[125] which confers to consumers the right to terminate the contract immediately. As per Article 12(5) DCD, another case constitutes the lack of conformity that impairs functionality, interoperability and other main performance features of the digital content. Last but not least, consumers have the right to terminate the contract from a temporal perspective. According to Article 16(1) DCD, consumers can terminate an indeterminate contract or one which cumulatively lasted for at least 12 months.

The termination of the contract also implies certain obligations on the supplier. First of all, suppliers shall take all measures to refrain from using the counter-performance and any other content provided by the consumer.[126] The question arises as to what is defined as counter-performance considering the lack of explained terminology in the Proposal.

In any case, there is a notable exception regarding content that has been generated jointly by the consumer and others who continue to make use of the content. In terms of personal data which can be part of the content, one can think of aggregated data used for service analysis for instance. DCD remains silent on defining who others are. This leaves room for a supplier to argue that other consumers generated content as well. Based on analysis of that data to observe the functionality of the app which is then used to improve the app means that all the content a former consumer generated is still made use of by others.

Secondly, suppliers have the obligation to retrieve the content provided by the consumer.[127] This matter is further discussed in Chapter 5.

Thirdly, after retrieving the content to the consumer, suppliers may prevent further use by making the content unavailable and disabling user account.[128] Another distinction is made between how the content was supplied: on a durable medium or not. In other directives,[129] the verb 'provided' is used in connection with durable medium while in DCD legislators chose for 'supplied'. Durable medium refers to a medium which enables consumers, similarly to paper form, to be in possession of relevant information to enable them to exercise their rights,

[125] Or at the time prescribed in the contract.

[126] Article 13(2)(b) DCD.

[127] Article 13(2)(c) DCD.

[128] Article 13(3) DCD.

[129] Consumer Rights Directive, Markets in Financial Instruments Directive (MiFID II) 2014/65/EU, Insurance Distribution Directive 2016/97/EU.

as required.[130] Furthermore, a durable medium must be able to store information aimed at users, ensure that the content will not be altered and accessible and it can be reproduced unchanged.[131] The European Court of Justice considers websites a durable medium.[132] By the same token, apps can also be seen as durable medium. However, the Proposal does not make the difference between tangible and non-tangible medium as in the Consumer Rights Directive. This causes tensions as CRD refers to digital content as goods.

[130] C-375/15 BAWAG PSK Bank v Verein für Konsumenteninformation.
[131] Ibid.
[132] Ibid.

5 Right to data portability

After the Commission proposed the DCD, the right to data portability (RTDP) specific to data protection was compared with the right of the consumer to receive the provided content back after the contract has been terminated. In order to understand the implications of RTDP for consumers and whether this is in dichotomy with the Proposal, we explain what the RTDP entails as defined in Article 20 GDPR:

> 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.

The RTDP is a two-sided right: it enables data subjects to receive a copy of their personal data and to transmit the data to another controller. A further classification is made in literature which indicates three distinct rights: rights to receive the data in a machine-readable format, the right to transmit the data to another controller and the right to transmit the data directly from controller A to controller B.[133] However, we consider that the distinction only based on the two types of rights more used in the academic discourse[134] fits this analysis in a better fashion.

Under Article 20(1), the personal data subject to RTDP must have been processed based on (explicit) consent or on the basis of a contract performance. Furthermore, the data must have been processed by automatic means.[135] The scope of covered personal data refers to data provided by the data subject. WP29 elaborates by making a distinction between types of data that fall under "provided by":[136] data actively and knowingly provided by the data subject and observed data provided by the data subject by virtue of the use of the service or the device[137] in comparison with inferred data. For the first type, we can think of name, e-mail, address filled in an online form whereas inferred data constitutes the profile created after the analysis of your shopping habits. With regards to the "observed data", WP29 considers that data collected through tracking and recording of the data subject falls under the scope of the

[133] Przemysław P. Polański, Data Portability, 3.

[134] Also the same distinction is made by the Article 29 Working Party (Guidelines on the right to data portability, 4 – 5); Zanfir, 'The right to Data portability in the context of the EU data protection reform'.

[135] Article 20(2) GDPR.

[136] WP29 RTDP Guidelines, 10.

[137] Ibid.

RTDP.[138] Most importantly, WP29 advises the term "provided by" to be interpreted broadly. The EU Commission expressed some concern regarding this advice since the scope of which personal data is concerned is too broad.[139]

Another aspect of the RTDP concerns the format of the data which shall be "structured, commonly used and machine-readable". This refers to files that are easily for machines to interpret such as XML, CSV or JSON.[140] Consequently, the PDF format which is easily comprehensible for human eyes is usually difficult for machines to comprehend.[141]

The data subject shall also be able to have the data transferred to another controller "without hindrance" which refers to any type of obstacle on the controller's side that prevents the data subject or the controller that receives the data from reusing, transmitting or having slow down access to the data.[142] In this regard, WP29 emphasizes the necessity of security of systems and networks which fall on the controller's obligations. Concerns have been expressed on this point concerning potential identity fraud or potential attacks to data in transition.[143] On the one hand, id frauds can pose high risks in case of free services offered by social media: if your personal account has been hacked and the hacker can provide enough credentials to prove that your profile belongs to him, he can download all your data. This becomes especially dangerous for users that have had online profiles for a major part of their lives. On the other hand, once personal data sent to the cloud is encrypted, the RTDP cannot be exercised anymore.[144] By ensuring adequate security controls for the personal data at all times, controllers respect the integrity and confidentiality of data.[145]

When the data subject chooses to transmit the data directly from one controller to another, this shall be technically feasible. However, as per Recital 68 GDPR, controllers are not obliged to have in place systems which are technically compatible. Last but not least, the RTDP shall be exercised without prejudice to rights and freedoms of other individuals. WP29 suggests that controllers shall develop tools to differentiate between personal data of the requesting data subject and other data concerning third parties.[146] Alternatively, third parties shall consent to

---

[138] Ibid.

[139] International Association of Privacy Professionals, 'European Commission, experts uneasy over WP29 data portability interpretation', <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/

[140] Polański, RTDP, 6. >

[141] Bozdag, 3.

[142] WP29, 'RTDP Guidelines', 15.

[143] Lucio Scudiero, 'Bringing Your Data Everywhere', 124 – 125.

[144] Ibid, 125.

[145] Article 5(1)(f) GDPR.

[146] WP29, 'RTDP Guidelines', 12.

the data transfer of their data.[147] In practice, this becomes an issue because controllers have to make an assessment concerning what criteria must be applied when classifying the content.[148] Another risk, especially for small and medium sized companies, arises when implementing Application Programming Interfaces (API) because this requires major investments[149] therefore the lack of resources of these companies might lead to improperly working APIs prone to security incidents.
Despite theoretical discussions being the blueprint of a solid and practical solution, for the RTDP this might not be the case. Unfortunately, through the nature of my job, I came across clear examples of companies which simply do not have the resources to answer to simpler requests such as the erasure of personal data.

As per Article 12 GDPR, data controllers must fulfill the request within one month. In case the request concerns a complex case, they must inform the concerned data subject that the response will be delayed to up to three months and the reasons for the delay. The request shall be free of charge for data subjects. WP29 underlines that controllers using APIs will only have a few cases in which they could justify a refusal to answer a RTDP request.[150] There are only two instances in which a request cannot be fulfilled: in they are manifestly unfounded or excessive and when having a repetitive character. These justifications have to be well-reasoned when sent to data subjects and documented for accountability purposes.

After describing the legal requirements for RTDP and some of the underlying issues, I will touch upon certain aspects that can be found at the overlap between RTDP as a data protection right and consumer law.

5.1 RTDP – a consumer law matter?

Besides the discussion on the relationship between competition law and RTDP, there is an ongoing dichotomy between assigning this right under data protection and consumer law.

5.1.1 Origins of RTDP

From a historical perspective, data portability is not a new concept: it first appeared in the "Bill of Rights for Users of the Social Web"[151] in 2007 which further influenced the creation

[147] Ibid.

[148] Polański, 'RTDP', 6.

[149] Polański, presentation at the Consumer Law in the Data Economy conference.

[150] WP29 'RTDP Guidelines', 15.

[151] Engin Bozdag, 'Data Portability', 1. Kurt Opsahl, 'A Bill of Privacy Rights for Social Network users', <https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users>, accessed 11 November 2018.

of the "Data Portability Project" whose aim was how to find practical solutions to data portability.[152]

At the same time, on a more philosophical level, RTDP stems from our digital persona, having its foundations in the free development of human personality.[153] Nowadays, individuals have their personality on Facebook in which they invested time and most importantly, valuable content[154] such as photos, check-ins, types of relationships, connections and even job history. Under these circumstances, RTDP becomes not only another data protection right but indeed empowers data subjects to transfer their digital persona wherever they want to. Albeit seeing the advantages of moving individuals' data from Facebook to new social media such as idka.com,[155] they still have several digital personalities online. For instance, as a consumer, it is most likely that an individual wants to transfer his or her "personality" from Amazon to bol.com.[156] Therefore, RTDP as a fundamental (human) right becomes even more important as it allows an individual's digital personalities to cross borders of a single website.[157]

In the European Union, the first type of portability was introduced by the Universal Service Directive,[158] which grants consumers the right to switch between mobile providers while keeping their mobile numbers. One of the early arguments for connecting RTDP with the right to privacy[159] and right to protection of personal data[160] has been discussed in light of the informational self-determination.[161] In brief, the individual shall have the right to choose another service provider for processing his or her data.

With this in mind, in the context of consumer protection, RTDP can be seen as ensuring consumer protection. Firstly, European legislation guarantees to consumers fair treatment. In the sense that a consumer is able to transfer her data by individual choice constitutes fair treatment. Basically, by complying with data protection law, the supplier[162] ensures a fair[163]

---

[152] Data Portability Project: <http://dataportability.org/>, accessed 11 November 2018.

[153] Gabriela Zanfir, The right to Data portability int he context of the EU data protection reform, 151.

[154] Tene, Me, Myself and I, 3.

[155] Idka aims to be a social platform that allows sharing and communicating with personal connections while keeping the data private, safe and owned by the user, <https://www.idka.com/en/>. Despite the Cambridge Analytica incident not affecting Facebook as a result of the social campaign "#deletefacebbok", some tech-savvy users started looking into new options for their digital persona.

[156] Biggest online retailer in the Netherlands: <https://www.bol.com/nl/>.

[157] Zanfir (n150), 159.

[158] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services.

[159] Article 7 European Charter of Fundamental Rights.

[160] Article 8 European Charter of Fundamental Rights.

[161] Zanfir, (n150), 152.

[162] Or in terms of data protection: data controller.

conduct towards its consumers. Secondly, with regard to having products that meet acceptable standards, services must be technically able to support a RTDP request. If this legal requirement is fulfilled, then in a broad sense, the product satisfies standardization requirements. Last but not least, the consumer must have a right of redress if something goes wrong. According to GDPR, the data subject has the right to lodge a complaint with a supervisory authority or to an effective judicial remedy.[164] Given these points, RTDP does not necessarily have to be conceived under consumer protection law. After all, the above shows one more opportunity for consumer organizations to make use of data protection law in order to address a consumer protection claim.[165]

5.1.2 RTDP and DCD

While observing the big picture of the connection between RTDP and consumer protection law aims, a more interesting situation arises when the detailed scope of concerned data in RTDP and DCD is analysed. A disclaimer should be made – this discussion does not aim to reach a definite conclusion about consumer protection clauses under DPD but intends to address tension points with data protection.

A major distinction between the RTDP and the right of retrieval concerns the timing for exercising the right. The latter can only be used by the data subject after the termination of contract whereas RTDP can be exercised at any point in time during the processing operations.

RTDP concerns data "provided by" the data subject and should be interpreted in a broad manner. Recital 39 DCD and Article 13(2)(c) DCD refer to the personal and non-personal data uploaded by the consumer, produced by the consumer with the use of the digital content or generated through the consumer's use of the digital content. In order to comply with this obligation, the supplier must *retrieve*[166] the aforementioned data to the consumer. In comparison with Article 20 GDPR, the focus here is on the supplier. Interestingly, the Commission used the word "retrieve"[167] which seems to be more powerful in obliging the supplier to check all its databases and systems in order to send all the concerned data to the individual. RTDP in GDPR makes reference to the data subject that should *receive*[168] her

[163] Substantive fairness means that a person is treated in accordance with the legal standards applying in a given context.

[164] Articles 77, 78 GDPR.

[165] See Rott, Data protection as consumer law: consumer organisations tried cases regarding unlawful privacy notices as a breach of unfair contract terms law.

[166] Emphasis added.

[167] 1. Get or bring (something) back from somewhere. 2. Find or extract (information stored in a computer) <https://en.oxforddictionaries.com/definition/retrieve>

[168] Emphasis added.

personal data. The wording shows that GDPR is centered around human rights, whereas DCD is a legislation focused on the supplier – consumer relationship. Furthermore, the wording emphasizes that the data subject's perspective who must have her rights enforced. At the same time, GDPR limits this right to only two legal bases for processing: based on consent and necessary for the performance of a contract. As widely acknowledged, these nuances lead to similar but not identical obligations[169] which will create more confusion for suppliers.

With regards to the data that has to be received by the data subject, Article 20 GDPR refers to personal data which has been provided to the controller.[170] Identical articles 13(2)(c) and 16(4)(b) DCD refer to *any other data produced or generated* through the consumer's use of digital content to the extent that this data has been retained by the supplier. In practice, what is the difference between these sets of data in the sense of the manner in which they were collected by the supplier? When referring to observed data that falls under the scope of RTDP, WP29 uses the example of a device that tracks raw data such as heartbeats.[171] Recital 39 DCD adds one more type of data i.e. uploaded. Whereas the DCD does not further explain what uploaded or produced means, some guidance can be found in Recital 15 DCD for generated content, which will most probably include personal data. Examples include music, video files, pictures, tweets, logs, posts, etc. This indicates that generated data refers to content explicitly created by consumers, which falls out of scope of the RTDP as it is not raw data or actively provided. The Commission used the wording "produced or generated". The definition of the word "produce[d]"[172] refers to generated content as explained in Recital 15[173] thus we can consider that there is no distinction between these terms. To sum up, DCD would extend the RTDP to created data by the consumer.

On the other hand, "uploaded" data refers to "a transfer from one computer to another, typically to one that is larger or remote from the user or functioning as a server."[174] The inclusion of the verb in Recital 39 seems to extend right of retrieval in a similar fashion as the RTDP. Based on the definition from the dictionary for "uploaded", it refers to actively and knowingly provided data by the data subject. This overlap between DCD and GDPR leads again to two different legal bases for exercising a right without adding any value for the consumers.

---

[169] Robert and Smit, 'The proposal for a directive on digital content', 13.

[170] See discussion in Chapter 2.

[171] WP29, 'RTDP Guidelines', 10.

[172] Make or manufacture from components or raw materials; Cause (a particular result or situation) to happen or exist. Oxford dictionary <https://en.oxforddictionaries.com/definition/produce>.

[173] In addition, synonyms for "generate" are "produce", "create".
Oxford dictionary, <https://en.oxforddictionaries.com/definition/generate>.

[174] Oxford dictionary, https://en.oxforddictionaries.com/definition/upload>.

Another point of tension between GDPR and DCD constitutes the scope of RTDP vs the right to retrieve all content provided by the consumer in light of the legal bases applicable to the processing of personal data. Whereas the RTDP applies only when processing is based on consent and when based on a contract, the WP29 still encourages good practices to be developed in relation to other legal basis "by following the principles governed by the RTDP".[175] However, strictly speaking, GDPR imposes legal obligations whereas WP29 makes recommendations on the implementation of data protection rules.[176] It remains to be seen in practice how controllers will deal with showing good practice in this sense considering the burden already brought by the implementation of the RTDP.

The legal bases for processing personal data that are usually applicable in a business context are consent, performance of a contract, legitimate interests and compliance with a legal obligation.[177] While the last mentioned is sufficiently clear in this context, DCD raises some questions concerning legitimate interests. Here DCD seems to extend the scope of GDPR and grant consumers a similar right to RTDP. The Court of Justice of the European Union made clear that economic interests of the controller cannot overcome fundamental rights of data subjects.[178] The rationale behind the exclusion of the legitimate interests as legal basis from the scope of RTDP is that the controller had already carried out a balancing test between its economic interest and fundamental rights of individuals. As a consequence, since DCD would extend the exercise of a similar right to retrieve data to a legal basis excluded by the RTDP, there will be greater confusion created when faced with complying with contradictory rules.

5.2 Practical implementations of RTDP

After having a theoretical discussion on the overlap of these rights and whether the RTDP should be dealt with under consumer law, I will briefly touch upon the practical issues that arise from these distinct rights to data portability. I am of the opinion that this discussion is essential in light of *lex ferenda* in order to ensure that technical obstacles do not stay allegedly in the way of exercising fundamental rights.

Firstly, the blueprint of the RTDP lies in being able to transfer data between controllers or to the consumer in machine-readable format. While this requirement can be satisfied as the controller sends the data in different formats to the receiver, it is of greater significance whether that data can be used for other purposes as desired by the data subject or authorized by the new controller.

[175] WP29, 'RTDP Guidelines', 8.

[176] Article 30(3) Data Protection Directive.

[177] Article 6 GDPR.

[178] C-131/12 Google Spain, para 67.

As mentioned previously, JSON – a data format, is widely used to store Internet of Things (IoT) data because of its flexibility which allows storage of diverse data with different structures.[179] However, most of the companies use closed proprietary systems[180] which are vertically integrated, meaning that it is increasingly difficult to combine them with third parties' systems.[181] This becomes an issue not only for harvesting big data and analytics[182] which require machines to have a common understanding of data formats but also for RTDP. Extensive discussions and initiatives[183] have expressed the need for well-defined data formats to ensure that the potential of IoT will be explored to the maximum.

Results from December 2017 stemming from a long term research investigating the user's privacy exposure[184] show that 7 out of 19 apps provide users with a practical mechanism to send a request to port their data, while 2 out of these 7 allow this via a web platform.[185] There are also differences in terms of making the request: one app allowed a request by e-mail whereas two others through sharing mechanisms only for some parts of the data.[186] Unfortunately, this shows how unprepared is also the MHA area for implementing the RTDP.

[179] JSON format manual, <http://jsonstudio.com/wp-content/uploads/2014/04/manual141/_build/html/iot.html>, accessed 11 June 2018.

[180] Ahlgren et al, 'Internet of Things for Smart Cities: Interoperability and Open Data', 53.

[181] Ibid.

[182] Milan Milenkovic, 'The Internet Of Things', 3.

[183] See BIG IoT: Bridging the Interoperability Gap of the Internet of Things – EU funded project aimed at establishing interoperability by defining a unified Web API for IoT platforms. <http://big-iot.eu/project/>; See also the Web of Things Working Group established by the World Wide Web Consortium (W3C) aimed at standardizing IoT interoperability thus countering the fragmentation of IoT. <https://www.w3.org/WoT/>.

[184] Achilleas Papageorgiou et al, 'Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice', 9390.

[185] Ibid, 9399.

[186] Ibid, 9400.

6 Conclusion

As also recognized by the EP, the European legislators are indeed faced with the challenging task of reconciling the fundamental rights approach with the economic reality.[187] Despite the drafting of GDPR being a very difficult assignment, its effects on other acts and areas of legislation started to emerge and are subject to heated debate.

This paper has shown that in the field of MHA, there are more blurred than clear lines between data protection and consumer protection. To begin with, a different classification for personal data and its purposes according to DCD in comparison with GDPR limits the scope of the Proposal. What is more, DCD seems to have become a *lex specialis* for GDPR whereas its aim was to complement data protection legislation.

On the topic of remedies, the abundance of conditions upon which consumers can exercise their rights leads to a very confusing picture. With the enactment of GDPR, consumers became more aware of their rights to protection of their data. However, awareness does not mean that consumers fully understand the rights. Consequently, the remedies from DCD contribute to the impaired understanding.

With regards to RTDP and the right to have the data retrieved in DCD, a similar phenomenon is observed. The timing requirements in DCD lead to confusion and extend the scope of the RTDP. It is noteworthy that the GDPR-specific conditions for exercising the RTDP only if personal data was processed based on two legal bases and the differentiation between produced, uploaded and generated in DCD increases the already difficult implementation of the RTDP for businesses.

To sum up, my research proves that DCD is an inconsistent piece of legislation which, while well-intended, leads to uncertainty. This is in line with what Clifford, Graef and Valcke[188] describe in their previous scrutiny: 'Despite being deliberate, the proposal, rather than representing an informed legislative choice, instead manifests an ill-informed understanding of data protection and privacy legislation and is a result of the complex legislative history related to the attempted harmonization of contract law formation at the EU level'.

One should not lose hope in the European legislators and their endeavor to protect consumers/data subjects from unfair commercial attitudes. That is why research should be

[187] Briefing on Data Protection, 1.

[188] Damian Clifford et al, 'Pre-Formulated Declarations of Data Subject Consent—Citizen Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections', 2018, 27. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126706>.

further conducted on aligning the discussed bodies of law. To draft a successful piece of hybrid legislation, more time should be spent on first understanding the overlap in data consumer law.

Table of references

Books

Hannah R. Marston, Shannon Freeman, Charles Musselwhite (eds), Mobile e-Health, Springer International Publishing AG, 2017.

Paul Chynoweth, Legal Research in the build environment: A methodological framework, University of Salford, <http://usir.salford.ac.uk/12467/1/legal_research.pdf>.

Paul Voigt, Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) – A practical guide, Springer, 2017.

Articles

Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis, 'Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice'.

Axel Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?', Journal of Intellectual Property, Information Technology and Electronic Commerce Law" Volume 2, Issue 8, 2017, 1 – 8.

Bengt Ahlgren, Markus Hidell, and Edith C.-H. Hgai, 'Internet of Things for Smart Cities: Interoperability and Open Data', IEEE Computer Society, 2016.

Cheng-Kai Kao, David M. Liebovitz, 'Consumer Mobile Health Apps: Current State, Barriers, and Future Directions', Clinical Informatics in Physiatry, Volume 9, Issue 5, May 2017, 106 – 115.

Chiara Crico, Chiara Renzi, Norbert Graf, Alena Buyx, Haridimos Kondylakis, Lefteris Koumakis and Gabriella Pravettoni, 'mHealth and telemedicine apps: in search of a common regulation', Special Issue, Journal of Cancer, 2018, 1-6.

Chris Jay Hoofnagle, Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price', UCLA Law Review, Volume 61, Issue 606, 2014.

Christine Prince, 'Do consumers want to control their personal data? Empirical evidence', International Journal of Human-Computer Studies, Volume 10, February 2018, 21 – 32.

Dan Svantesson and Roger Clarke, ‘A best practice model for e-consumer protection’, Computer Law Security Review, Volume 26(1), 2010, 31 – 37.

Dan Svantesson, ‘Enter the quagmire – the complicated relationship between data protection and consumer protection law’, Computer Law & Security Review, Volume 34, 2018, 25 – 36.

Engin Bozdag, ‘Data Portability under GDPR: Technical Challenges’ (Draft version, currently under review), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3111866>.

Lothar Determann, ‘No one owns data’, Legal Studies Research Paper Series, Research Paper No. 265, 2018.

Mary Sharp, Declan O’Sullivan, ‘Mobile Medical Apps and mHealth Devices: A Framework to Build Medical Apps and mHealth Devices in an Ethical Manner to Promote Safer Use – A Literature Review’, Informatics for Health: Connected Citizen-Led Wellness and Population Health, 2017, 363 – 367.

Milan Milenkovic, ‘The Internet of Things: A Case for Interoperable IoT Sensor Data and Meta-data Formats’, Ubiquity Symposium, Association for Computing Machinery, November 2015.

Natali Helberger, Frederik Zuiderveen Borgesius, Agustín Reyna, ‘The Perfect Match? A closer look at the relationship between EU Consumer Law and Data Protection Law’, Common Market Law Review, Volume 54, 2017, 1427–1466.

Peter Rott, ‘Data protection law as consumer law – How consumer organisations can contribute to the enforcement of data protection law’, European Consumer and Market Law Review, Issue 3, 2017, 113 – 119.

Rishi Duggal, Ingrid Brindle, Jessamy Bagenal, ‘Digital healthcare: regulating the revolution, Editorial’, The British Medical Journal, January 2018, <https://doi.org/10.1136/bmj.k6>.

Romain Robert, Lara Smit, ‘The proposal for a directive on digital content: a complex relationship with data protection law’, Academy of European Law, April 2018, <https://doi.org/10.1007/s12027-018-0506-7>.

Working Papers

European Data Protection Supervisor, 'Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', March 2014.

Information Commissioner's Office, 'Big data, Artificial Intelligence, machine learning and data protection', March 2018.

Marco B.M. Loos, 'Full harmonisation as a regulatory concept and its consequences for the national legal orders. The example of the Consumer rights directive', Centre for the Study of European Contract Law Working Paper Series No. 2010/03.

Prof. ALK dr hab. Przemysław P. Polański, 'Some thoughts on data portability in the aftermath of Cambridge Analytica scandal', April 2018 (presented at the Consumer Law in the Data Economy conference, Amsterdam, 13th April 2018).

Lucio Scudiero, 'Bringing Your Data Everywhere', 124 – 125.

Legislation/proposals for legislation/Guidelines

Annex II Commission Work Programme 2015, <https://ec.europa.eu/info/sites/info/files/cwp_2015_annex_ii_en.pdf>

Article 29 Data Protection Working Party, 'Letter of the chair on mHealth', April 2017.

Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', August 2018.

Article 29 Working Party, 'Guidelines on the right to data portability', April 2017.

Article 29 Working Party, Guidelines Consent for the purposes of Regulation 2016/679, April 2018.

Briefing Contracts for the supply of digital content and digital services. EU Legislation in progress, February 2018.

Commission Staff Working Document, 'Impact Assessment Accompanying the document Proposals for Directives of the European Parliament and of the Council (1) on certain aspects concerning contracts for the supply of digital content', COM/2015/0634 final.

Consolidated Version of the Treaty on European Union, 2007.

Council of the European Union, 'General Approach - Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (First reading)', June 2017.

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

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.

European Commission, 'Code of Conduct on privacy for mobile health applications', June 2016, <https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps>.

European Data Protection Supervisor, 'Data Protection', <https://edps.europa.eu/data-protection_en>.

European Parliament Briefing, 'Contracts for the supply of digital content and personal data protection', May 2017.

European Parliament, 'Report on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (COM(2015)0634 – C8-0394/2015 – 2015/0287(COD))', November 2017, <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0375&language=EN>.

Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM(2015) 634 final.

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).

Case-law

C-375/15 BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG v Verein für Konsumenteninformation.

Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others. Court of Justice of the European Union.

Websites, online presentations

Andrew Beattie, 'How YouTube Makes Money Off Videos (GOOG)', <https://www.investopedia.com/articles/personal-finance/053015/how-youtube-makes-money-videos.asp>.

Brussels Privacy Hub Meets the Author series: Dr Frederik Zuiderveen Borgesius and Agustín Reyna, 'The relationship between EU consumer law and data protection', <https://www.youtube.com/watch?v=9DNIGNkFj4I>.

Christiane Wendehorst, 'Proposed Digital Content Directive and its Implications for the Data Economy', presentation at the XXXII Nordic Conference on Legal Informatics, 13 November 2017.

CNET, 'These were the weirdest products at CES', 12 January 2018, <https://www.cnet.com/pictures/ces-2018-weirdest-gadgets/34/>.

Computers, Privacy and Data Protection Conference 2018. 'The Perfect Match? A Close Look At The Relationship Between Consumer Law And Data Protection Law', <https://www.youtube.com/watch?v=nb58BVGy5Og>.

Dave Muoio, 'Study: Many health apps insecure, do not conform to EU privacy requirements', <https://www.mobihealthnews.com/content/study-many-health-apps-insecure-do-not-conform-eu-privacy-requirements>.

Ellen Simon, 'How Instagram makes money', <https://www.investopedia.com/articles/personal-finance/030915/how-instagram-makes-money.asp>.

European Commission. 'Digital Single Market Strategy', <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market>.

European Parliament, the Council and the European Commission, 'Joint Declaration 2018', <http://www.europarl.europa.eu/oeil/popups/thematicnote.do?id=2063000&l=en>.

Freeletics. 'About us', <https://www.freeletics.com/en>.

International Association of Privacy Professionals, 'European Commission, experts uneasy over WP29 data portability interpretation', <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/>.

International Association of Privacy Professionals, 'WP29 data portability interpretation spooks European Commission', <https://iapp.org/news/a/wp29-data-portability-interpretation-spooks-european-commission-legal-analysts/>.

Joe Hindy, '10 best health apps for Android', <https://www.androidauthority.com/best-health-apps-for-android-668268/>.

Kurt Opsahl, 'A Bill of Privacy Rights for Social Network users', <https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users>.

Laura Drechsler, Workshop Summary Brussels Privacy Hub Meets the Author series: Dr Frederik Zuiderveen Borgesius and Agustín Reyna, 'The relationship between EU consumer law and data protection', <https://brusselsprivacyhub.eu/publications/ws13.html>.

Martin Abrams, 'The origins of Personal Data and its Implications for Governance', The Information Accountability Foundation, 6 – 11<http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>.

POLITICO, 'Politicians follow in Facebook's footsteps on mass data collection', <https://www.politico.eu/pro/facebook-cambridge-analytica-data-protection-privacy-brexit-trump-vote-leave-ucampaign/?utm_source=POLITICO.EU&utm_campaign=185bea1947-EMAIL_CAMPAIGN_2018_04_09&utm_medium=email&utm_term=0_10959edeb5-185bea1947-190299577>.

Techopedia, 'Mobile Application', <https://www.techopedia.com/definition/2953/mobile-application-mobile-app>.