SCALES

Designing regulatory and institutional framework to balance public interest and individual liberties in the use of data analytics

NWO | TARGET holding

Realizing the Full Potential of the Right to Data Portability:
Using Data Protection for Healthcare Innovation

Realizing the Full Potential of the Right to Data Portability:

Using Data Protection for Healthcare Innovation

Co-authored by:
Dr. Mark Leiser
Lexo Zardiashvili, LLM
Dr. Francien Dechesne

SCALES is a research project funded by The Netherlands Organization for Scientific Research programme on "Responsible Innovation", with several private and public partners participating. The overarching research question of SCALES is how to strike a balance between individuals, public and private data-producers, data controllers and data-processors. The project aims to inform the regulatory and institutional landscape, allowing for optimal utilization of data analytics to serve the interests of governments, companies, and users, while optimally safeguarding individual rights and liberties. To achieve this objective, case studies have been conducted with the partners in the field of energy, law enforcement, and data analytics.

Target Holding is a private partner within the SCALES project, specialized in data analytics, currently working on the development of a digital personal health environment (hereafter PHE) – "*IkDus*". A PHE is an online platform, where users can keep medical information provided by their care providers and store data from fitness apps that monitor health and exercise.

This report has been produced by researchers at the eLaw Center for Law and Digital Technologies at Leiden University. In doing so, our understanding of the business processes of *IkDus* is based on the information provided by Target Holding and its associates, as well as information available from public sources.

2019

Leiden, The Netherlands

Table of Contents

Introduction

The collection and analysis of vast amounts of data in an increasingly networked world holds great potential for both enterprise and the public sector. Data-driven products and services are developed in a wide variety of domains; for example, for the purposes of scientific research and discovery, to increase safety and security, to improve sustainability, to increase efficiency, to enhance mobility, to protect health and to improve quality of life. At the same time, the increasing availability and the capacity to analyze data can threaten individual liberties such as autonomy and privacy.

Personal data, and the insights derived from it, have become valuable resources in the emergent data economy. In order to incentivize innovation and strengthen the data subjects' control over their own data, Article 20 of the EU's General Data Protection Regulation (GDPR) provides for a new right to data portability (hereafter, Rt2DP) that, under certain conditions, enables data subjects, where technically feasible, to receive their personal data or to transmit directly from one controller to another.

The Rt2DP empowers users wishing to change suppliers, or to move from one product or brand to another, without losing access to their historical data. In addition, Rt2DP extends to the porting of data from one data controller to a third party provider who can then merge user-provided data with their own for additional data subject insights into their behavior. For example, activity tracking, when compiled with medical data, could encourage users into doing more exercise and making better lifestyle choices, drastically reducing financial and time burdens on users, businesses, researchers, healthcare providers, insurers, and/or the state. Furthermore, data subjects can migrate their data to their health providers for progress reports or to inform researchers about statistical anomalies (i.e. cancer clusters).

Although the development of innovative personalized healthcare environments (PHEs) like *IkDus* is actively encouraged **[1]**, their very nature raises legal questions about the processing of health data. In this report, we critique the role of the GDPR's Rt2DP in light of our understanding of the *IkDus* platform.

1. *IkDus* – Universal digital health profile

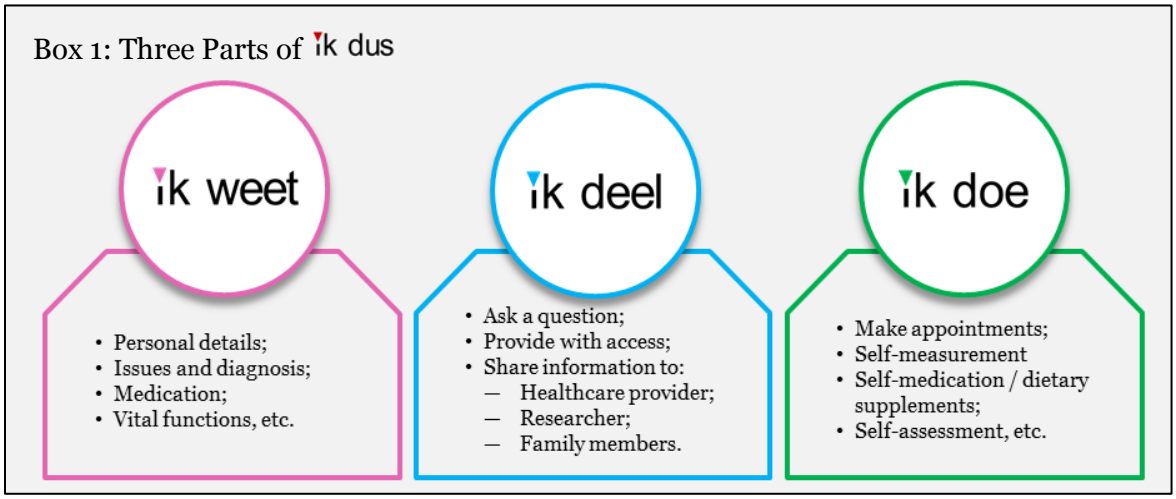
1.1. At present, most individuals share various types of health data with different healthcare professionals. For example, a patient with multiple sclerosis may visit a general practitioner (hereafter GP), but also a neurologist, a urologist, a rehabilitation hospital, a homecare specialist, a home-adaptation specialist and many other types of support. All are instrumental in developing a plan for the patient's care. In a perfect world, all support would be delivered in a coordinated way. However, in practice, many healthcare providers are unaware of other treatments and care plans patients rely on. This can result in a "spider-web" of services and healthcare provisions.

1.2. *IkDus* ("Dat ben ik dus" *(Dutch)* – "that is me") is an initiative to support patient care and medical research. It is a centralized platform for maintaining the personalized health profiles of individuals living in The Netherlands. It processes various forms of patient health data (medical symptoms, diagnoses, medication, etc.) from various healthcare providers, as well as data concerning their lifestyle (e.g. data from wearables - heartbeat, steps, etc.), nutrition (e.g. diet apps - calories, hydration, etc.) and family (e.g. family history of medical issues).

1.3. *IkDus* will apply machine learning (ML) to the data compiled in the platform in order to predict future health developments and to provide evidence-based, personalized lifestyle or medication advice to users. By applying ML, *IkDus* strengthens the informational awareness of users have over their future health and to optimize their healthcare plans.

1.4. *IkDus* is made up of three parts: *IkWeet, IkDoe*, and *IkDeel*.

Box 1: Three Parts of ik dus



1.5. *IkWeet* makes information available for the users. *IkDoe* allows users to control, manage and make use of information; for example, for the purposes of measuring the progress or the effectiveness of dietary supplements. *IkDeel* provides the means for digital communication with healthcare providers (or researchers) and enables a patient to ask a

question or to provide a preferred physician with access to their health profile (or parts of it). Users will have relevant information regarding their health (*IkWeet)* so to help make informed decisions about their health *(IkDoe*) and shared with family members, healthcare professionals, or researchers (*IkDeel*).

2. The right to data portability

2.1. The Rt2DP has three components: The (1) right to receive the personal data concerning him or her (2) in a structured, commonly used and machine-readable format, (3) a right to transmit those personal data directly to another controller, without hindrance and where technically feasible.

2.2. The Rt2DP explicitly gives the data subject the right to receive (and not just access) personal data concerning him or her.

***Box 2** – Rt2DP - Article 20 (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…"

2.3. The right mandates that data is provided to the data subject in a format that is (i) structured, (ii) machine-readable and (iii) commonly used; therefore, it goes further than the Article 15 (right of access). When users receive data in generic formats, for example, a PDF or a ZIP file, they often face difficulties reusing those data. Hence, data in an appropriate format for further processing is a prerequisite for portability. First, to comply with the format requirement, data must have a specific structure; for example, to be stored in a database or in specific files (e.g. JSON or CSV files). This is to enhance the possibilities for reuse and/or coupling. Second, the format should be machine-readable, so it allows software applications to easily identify, recognize and extract specific data (e.g. CSV and XML files). Third, it should be a commonly used format. However, what formats are "commonly used" can differ between sectors. For example, the music sector uses e.g. MIDI and MusicXML while healthcare uses ODM, FHIR, etc. In addition, interoperability may be seen as an additional non-mandatory requirement adding to the description of the format requirement in Article 20.

2.4. Format requirements (and non-mandatory interoperability) allow data subjects to enforce their **right to transfer** their data to another data controller. Data transfers should be "without hindrance" from the initial controller. Examples of measures that can create hindrance include a lack of interoperability of formats, asking fees for delivering data, a lack of access to a preferred data format, deliberate obfuscation of datasets, excessive sectorial standardization, accreditation demands, etc.

Box 3 *- Article 20 (2) of the GDPR*

"In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible."

2.5. The Article 20(2) component provides that data should be able to be directly transmitted from one controller to another. This can be fulfilled by making an API available, or by using standard protocols. The text of Article 20 limits the obligation of data controllers to transfer the data to the cases when it is "technically feasible." However, there is no clear definition of what technically feasible mean. The European Banking Federation (EBF) suggests the following solution: if a data controller claims that a transfer is not technically feasible, it has to prove this. If it fails to do so, portability should be facilitated.

3. Limitations to the right to data portability

3.1. By enabling data subjects to receive their personal data and transfer to the data controllers of their own choosing, the Rt2DP can be seen as an important step to data subjects taking control over their own digital identities. On the other hand, the data portability right is not absolute. The following paragraphs provide an outline of its limitations.

3.2. Rt2DP applies only if following cumulative conditions are met:

1. Data concerning a data subject - for Rt2DP to apply, there must be a connection between the data and the identity of an individual. This suggests that anonymous data is excluded from the scope of Rt2DP; on the other hand, this situation is certainly fluid and subject to change, especially if the data subject provides additional information enabling his/her re-identification.
2. Data is provided to a controller by a data subject – Data can be provided by a data subject *actively* or *passively*. Data that is *actively provided* by data subject is usually data provided at the first interaction with the data controller e.g. personal information, e-mail addresses, telephone numbers, etc.). Data that is *passively* provided by the data subject is sometimes referred to as 'observed data' and usually includes behavioral data, or data gathered by observing the data subject's behavior (e.g. raw data of steps processed by wearables, heartbeat recorded by the app, etc.). However, the Rt2DP cannot be used to port data that is the result of *analysis* by a data controller. Therefore, the data controller would not be subject to port any medical diagnosis. As different interpretations of the term "provided data" could result in widely different amounts of data, it is unsurprising that this is one of the most disputed and critical aspects of Rt2DP's applications.

Box 4 *– Rt2DP - Article 20 (1)*

"The data subject shall have the right… 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."

3. Processing based on consent or for performance of a contract – This is one of the most important aspects of the data portability right. The data subject can only ask for their personal data via the portability right when it has been provided to the subject data controller through consent under Article 6(1)(a), or for performance of a contract under Article 6(1)(b). If the data subject wishes to port health data, a form of special category sensitive data, then the data should have been provided to the subject data controller through the higher standard of 'explicit consent' under Article 9(2). Any data relating to a data subject that is processed on any other legal basis will not be subject to the data portability right and the subject data controller can refuse to comply with the data subject's consent.

Box Box 5: cation of Rt2DP – condition of processing grounds ☑ Rt2DP applies ⊗ Rt2DP does not apply

6 grounds of processing (Article 6):	10 conditions of processing special categories of data (Article 9(2)):
☑ Consent	☑ Explicit Consent
☑ Contract	⊗ Legal obligation (employment, social security, etc.)
⊗ Vital Interest	⊗ Vital interest
⊗ Legal obligation	⊗ Legitimate non-profit activities (political, philosophical, etc.)
⊗ Task in Public interest	⊗ Data is manifestly public
⊗ Legitimate interest	⊗ Legal claims
	⊗ Substantial public interest
	⊗ Necessary for medical diagnosis, treatment, social care, etc.
	⊗ Public health
	⊗ Research and statistics

4. The processing is carried out by automated means – this excludes processing that is based solely on manual means.

Box 6 *– Rt2DP - Article 20 (4)*

"…shall not adversely affect the rights and freedoms of others"

5. Applying the Rt2DP must not adversely affect the rights and freedoms of others – Applying the Rt2DP might compromise or conflict with a third party's rights; for example, when a data subject requests their family's medical history. This data not only relates to the data subject, but also to members of their family. The Rt2DP could be restricted if it could have significant consequences for the business of a data controller; for example, porting would entail excessive implementation costs.

3.3. The following sections discuss how the Rt2DP can be used to facilitate the development of the *IkDus* platform. We examine the components of the Rt2DP and qualifications to the right. As most of the qualifications can be disputed, it is important to note that our interpretation of its wording is fluid and is subject to change. Interpretations could be broader or narrower, depending on future court rulings and/or guidance from data protection regulators.

4. Application of data portability right to *IkDus*: Known Knowns

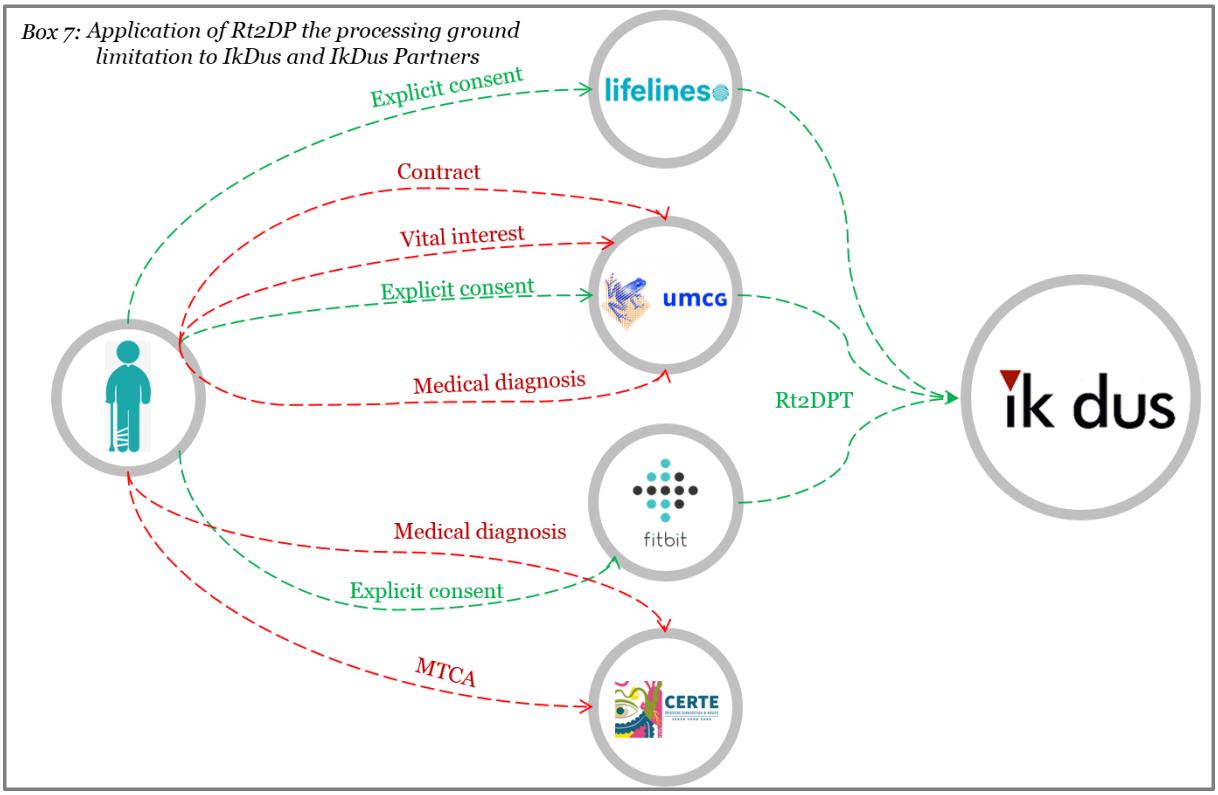
4.1. As the Rt2DP enables data subjects to transfer personal data from one controller to another, it is clear that Rt2DP can be used to facilitate the transfer of data into the *IkDus* platform, and contribute to *IkDus's* overall objective of developing a digital health environment. However, much of the health data relating to a data subject will not be subject to a data portability request.

4.2. It is important to understand the Rt2DP's limitations. Processing health data requires a much higher threshold of data subject consent than other forms of personal data. In fact, the GDPR bans processing sensitive data altogether, unless certain conditions have been satisfied. Even if one of the grounds of processing sensitive data from this exhaustive list is satisfied by a data controller, the data portability right would only apply to data processed on the grounds of 'explicit consent'. For example, under Article 9(2)(c) health data can be processed if the processing is necessary to protect the vital interests of the data subject. This might occur when a data subject is not able to give consent (i.e. a patient lying in a diabetic coma). This information is important health data but would not be included in the execution of a portability request. It was not processed through 'explicit consent'. *IkDus*'s partners cannot be bound or forced to transfer data collected under any other ground than 'explicit consent'. To help conceptualize this limitation, we have provided three examples to explain how this works in practice:

- When acting as a research institute, UMCG will be processing data through the 'explicit consent' of a research participant. Accordingly, the data subject will have the right to port this data to *IkDus*.
- If a patient attends UMCG after an accident leaves them unconscious, UMCG will likely process personal data on grounds other than consent or performance of a contract. A patient left unconscious after a car accident would not be able to provide 'explicit consent' to treatment. In this case, any processing undertaken will likely be in "the vital interest" of the data subject. Much of the data gathered will not be subject to the Rt2DP.
- If a patient contacts UMCG to get tested for HIV, data will be processed on the grounds of "necessary for medical diagnosis". A data subject does not have the right to transmit this data to *IkDus*.

Processing health data without 'explicit consent' is permitted when there is a lawful basis for doing so; for example, processing may be required under the Dutch Medical Treatment Contract Act, or for performance of a contract with a health professional (i.e. psychotherapist).

Box 7: Application of Rt2DP the processing ground limitation to IkDus and IkDus Partners



4.3. Another limitation to the Rt2DP is that the data subject has a right to port only the data that he/she directly or indirectly provided to a controller. This excludes all the data that is derived or inferred by the data controller.

4.4. "Data directly provided" is data usually provided *actively* by the data subject upon the first contact with the data controller. This will likely include personal information such as name, address, e-mail, etc.

4.5. In some circumstances it will be hard to distinguish "observed data" (data indirectly provided by data subject through his/her behavior) from "inferred data". There are situations where the distinctions clear-cut. For example, consider the case of a fitness wearable device, like FitBit. A user's heartbeat is clearly observed data and must be ported, if requested by the data subject. However, a profile created by FitBit (to offer a user personalized workout plans) is "inferred data" and FitBit cannot be obliged to port this data to another controller. We have provided three examples to help explain:

- Outcomes from a patient health assessment (including any medical diagnosis, the analysis of blood samples, etc.) inferred by the data controller from the information provided by the patient are excluded from the Rt2DP. CERTE, for example, cannot be

obliged by a data subject to port the outcomes of analysis done on blood samples provided by its data subjects.

- Similarly, research participants cannot use the data portability right to request that Lifelines Biobank port the results of a health assessment based on the data subjects answers to a questionnaire.
- Inferred data would also include remarks *about* the data subject; for example, when a doctor examines the patient and writes "symptoms of bronchitis" in their file.

4.6. It is important to note that medical diagnosis or analysis of blood samples will fall under the scope of the Rt2DP when outcomes of a health assessment are provided by the data subject to the data controller (rather than derived from the latter). This includes situations when a patient discloses information to his doctor; for example, about his/her chronic illness and later processes this as data provided by the data subject.

5. Application of the data portability right to *IkDus*: Known Unknowns

5.1. In certain situations, it is impossible to tell where the line is between “observed” and “derived” data. "Reputation scores" are often acquired by members of online marketplaces like Airbnb. Similar problems might arise in the cases of fitness wearables and health apps. The Article 29 Data Protection Working Party (hereafter A29WP) **[3]** recommends a broad interpretation of the term "data provided by data subject". However, the European Commission experts have criticized this approach as too data subject centric.

5.2. Another uncertainty relates to the grounds of processing used by the partners of *IkDus*. There may be situations where two or more conditions for processing health data are interconnected; for example, when a patient enters into a contract with a health professional, where the latter provides a medical diagnosis as a service and asks for ‘explicit consent’ for processing the data of the data subject. It is subject to interpretation which ground a data controller uses for processing.

5.3. Apart from the legal constraints of the Rt2DP, one of the challenges faced by *IkDus* is how to convince their users to exercise their right. Data portability as a service (hereafter DPaaS) has been posited as a potential solution to this problem. In a DPaaS relationship, a data subject would authorize *IkDus* - a DPaaS provider - to exercise the Rt2DP in his/her name and to demand that his/her data be sent directly to a third party or to the DPaaS provider itself. In this way, data subjects could have their data ported to their preferred provider. The GDPR can be interpreted in a way that facilitates these kinds of contracts. The A29WP has explicitly stated that it foresees these kinds of relationships emerging in the future. In addition, several Data Protection Authorities have stated that it is legal for a data subject to authorize a third

party the right of access in his/her name. This argument could be extended to all other data subject rights, including the Rt2DP.

5.4. If acting as a DPaaS provider, *IkDus* should take into consideration other aspects of the Rt2DP that might pose additional challenges.

1. Data controllers are required to implement an authentication procedure to ascertain the true identity of the data subject requesting the porting.
2. DPaaS providers handling portability requests on behalf of a data subject must consider how long it takes for the target data controllers to respond to the DPaaS request on behalf of the data subject.
3. DPaaS providers must be prepared for situations arising where the target data controller rejects the request or charges fees for porting data.
4. A DPaaS provider must ensure it provides a secure platform for the transmission of the data.

5.5. While not explicitly stated, the GDPR encourages data controllers to provide data to data subjects through Application Programming Interfaces (hereafter API). This interpretation provided by the A29WP, is a recommendation and not hard law. The theory is that APIs could enable *IkDus* users to transfer data from Fitbit in real-time.

6. Beyond Rt2DP and unknown unknowns

6.1. Because the GDPR obliges data controllers to transfer data (specifically the transfer of data in a specific format, without hindrance, etc.), it limits the Rt2DP when its exercise would disproportionally intervene within the right of the subject data controller to do business. Therefore, wherein data controllers are willing to share all their user data, regardless of the Rt2DP's qualifications, we believe there is no provision for preventing data controllers from doing so. For example, if UMCG is willing to share data processed on the grounds of "protecting vital interests of data subject" or where CERTE derives an outcome from an analysis of blood samples, they can still choose to legally transfer this data to *IkDus*, upon the request of a data subject. In fact, if they are willing and the data subject requests it, they can transfer *any* personal data to a new controller.

6.2. Although this might enable large data transfers, it must be understood that this does not extend the scope of the Rt2DP. In the scenario above, data subjects would not get the right to request data in a machine-readable, structured and commonly used format. Furthermore, nothing stops a data controller from charging for these type of data transfers and controllers can legally create hindrances to transfer or refuse to port the data at all. However, using generic file formats like PDF to transmit data could still provide valuable insights to both the user and *IkDus* partners.

Recommendations

Recommendation #1: To fully understand what data is likely to be ported upon a data portability request, *IkDus* should analyze data samples from their partners. This will help distinguish the data transmitted by its users and the data which controllers are not obliged to port.

Recommendation #2: To take full advantage of the data portability right, *IkDus* should encourage partners to process personal data on the grounds of 'explicit consent'.

Recommendation #3: *IkDus* should take legal advice about compliance with national legislation that may influence the interpretation of what it means to enter a medical contract.

Recommendation #4: *IkDus* must be aware that it becomes a data controller upon receipt of personal data transmitted to it after a data subject makes a Rt2DP request. It must comply with all the requirements of the GDPR and national data protection legislation. We recommend a thorough analysis of the compliance with all relevant data protection rules.

Recommendation #5: *IkDus* should clearly state the purpose of the new processing before any request for transmission of the portable data.

Recommendation #6: *IkDus* should provide data subjects with complete information about the nature of personal data relevant for the performance of its services. This will allow users to limit the unnecessary duplication of personal data and minimize risks for third parties.

Recommendation #7: *IkDus* has to ensure that the ported data is relevant for its services and its data processing is not excessive.

Recommendation #8: *IkDus* should develop technical and organizational measures for ensuring sensitive health data is secured with the latest technology, and develop a plan to ensure data remains secured with the state of the art technical and proper organizational measures.

Recommendation #9: For a proper analysis of the risks related to the processing of sensitive health data, *IkDus* should conduct a Data Protection Impact Assessment. (DPIA).

Recommendation #10: If not already done so, *IkDus* should appoint a data protection officer (DPO).

Recommendation #11: As a data controller, *IkDus* should be aware that the data subject might exercise their Rt2DP against *IkDus* and request data to be ported to another party.

Appendix 1 - *IkDus* Partners

Creating universal, or centralized, or personalized digital health profiles requires aggregating data from various sources. These sources include actors (GPs, hospitals, healthcare providers and research institutions) and applications (wearables, fitness and diet apps). By sharing data, partners can benefit from access to the *IkDus* platform. If their patient authorizes access, healthcare providers can get access to a large amount of data. Several healthcare research institutes and healthcare providers have indicated that they are willing to participate in the development phase of *IkDus*. The partners involved in preliminary talks on participation in the *IkDus* project (hereafter the *IkDus* partners) are:

i. Lifelines Biobank is a longitudinal cohort study collecting data and samples from over 167,000 participants over a period of thirty years. The Lifelines cohort comprises residents of the northern parts of The Netherlands covering three generations of data subjects: children, adults and the elderly. Several physical measurements are taken and recorded and questionnaires are filled out by the participants. These make up a significant percentage of all the data collected.

ii. CERTE is an organization for the development of integral medical diagnostics and for providing advice for first and second-line healthcare. Through laboratory research, functional testing and imaging diagnostics, CERTE delivers medical diagnostics for healthcare providers and their patients. CERTE is usually asked by a GP, a medical specialist or another healthcare provider, to perform analysis on the material of patient's body (blood, sputum, urine, feces, etc.) and report back to the physician(s) of the patient.

iii. The University Medical Center Groningen (UMCG) is one of the largest hospitals in The Netherlands and is the largest employer in the north of the country. Two of UMCG's core tasks are providing patient care and participating in scientific research. The UMCG offers care to patients who need complicated examinations and/or treatments, and to those who suffer from a rare disease or multiple disorders. For some complex cases, the UMCG is the only hospital in The Netherlands capable of treating patients.

iv. These partners appear willing to volunteer data to the platform, but *IkDus* is not limited by this list. *IkDus* can aggregate data from wearables (i.e. FitBit and Apple Watch), as well as data from GPs and other healthcare providers, etc.

Notes and References

1. The government of The Netherlands is encouraging the development of personalized digital healthcare environments (PHEs). The Dutch Act on the Client's Rights in Electronic Data Processing in Healthcare (Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg) sets minimum requirements for healthcare service providers to enable safe, reliable, user-friendly products allowing patients to safely compile and share their health data online. While acknowledging the importance of the compliance of the *IkDus* platform with the Dutch regulations in the healthcare domain, the scope of this report does not cover analysis of domestic legislation.
2. The Article 29 Working Party was an advisory body that provided expert (non-binding) advice regarding the implementation of the data protection rules. After the GDPR entered into force, the European Data Protection Board (EDPB) replaced the Article 29 Working Group to become the European Union's independent data protection authority.

Bibliography

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), available at: http://data.europa.eu/eli/reg/2016/679/oj
2. Helena Ursic, "Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control"(2018), 15:1 SCRIPT-ed 42, available at: https://script-ed.org/?p=3542;
3. Article 29 Data Protection Working Party, "Guidelines on the Right to Data Portability" (2017), available at: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf;
4. European Banking Federation, "European Banking Federation's Comments to the Working Party 29 Guidelines on the Right to Data Portability" (2017), available at: https://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.._.pdf;
5. Paul De Hert and others, "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services" (2018), Computer Law & Security Review, available at: https://www.sciencedirect.com/science/article/pii/S0267364917303333?via%3Dihub;
6. Lucio Scudiero, "Bringing Your Data Everywhere: A Legal Reading of The Right to Data Portability" (2017), 3 European Data Protection Law Review, available at: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/edpl3&section=21;
7. Inge Graef and others, "Data Portability and Data Control: Lessons for an Emerging Concept in EU law" (2018), 10 German Law Journal, 1359, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071875.