KADİR HAS UNIVERSITY
GRADUATE SCHOOL OF
SCIENCE AND ENGINEERING
PROGRAM OF
MANAGEMENT INFORMATION SYSTEMS

APPLICATION OF THE RIGHT TO DATA PORTABILITY: A TECHNICAL AND MANAGERIAL PERSPECTIVE

ALP ERKMEN

Master of Science Thesis

ISTANBUL, JANUARY 2019

APPLICATION OF THE RIGHT TO DATA PORTABILITY: A TECHNICAL AND MANAGERIAL PERSPECTIVE

ALP ERKMEN

MASTER'S THESIS

Submitted to the Graduate School of Science and Engineering of
Kadir Has University in partial fulfillment of the requirements for the degree of
Master of Science in Management Information Systems

ISTANBUL, JANUARY 2019

DECLARATION OF RESEARCH ETHICS /
METHODS OF DISSEMINATION

I, Alp Erkmen, hereby declare that;

- this Master's Thesis/Project/PhD Thesis is my own original work and that due references have been appropriately provided on all supporting literature and resources;
- this Master's Thesis/Project/PhD Thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- I have followed *Kadir Has University Academic Ethics Principles* prepared in accordance with *The Council of Higher Education's Ethical Conduct Principles*.

In addition, I understand that any false claim in respect of this work will result in disciplinary action in accordance with University regulations.

Furthermore, both printed and electronic copies of my work will be kept in Kadir Has Information Center under the following condition as indicated below (SELECT ONLY ONE, DELETE THE OTHER TWO):

The full content of my thesis/project will be accessible only within the campus of Kadir Has University.

ALP ERKMEN

DATE 11.01.2019

KADİR HAS UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

ACCEPTANCE AND APPROVAL

This work entitled APPLICATION OF THE RIGHT TO DATA PORTABILITY: A TECHNICAL AND MANAGERIAL PERSPECTIVE prepared by ALP ERKMEN has been judged to be successful at the defense exam on 04.01.2019 and accepted by our jury as MASTER OF SCIENCE THESIS.

APPROVED BY:

Assoc. Prof. Dr. Mehmet Nafiz AYDIN (Advisor) .....
(Kadir Has University)

Assoc. Prof. Dr. Ahmet Salih BIÇAKCI (Co-advisor) .....
(Kadir Has University)

Assoc. Prof. Dr. Nazım Ziya PERDAHÇI .....
(Mimar Sinan Fine Arts University)

I certify that the above signatures belong to the faculty members named above.

.....

Assoc. Prof. Dr. Ebru Demet AKDOĞAN
Graduate Institute of Science and Engineering

TABLE OF CONTENTS

Contents

APPLICATION OF THE RIGHT TO DATA PORTABILITY:
A TECHNICAL AND MANAGERIAL PERSPECTIVE

ABSTRACT

European Union's General Data Protection Regulation provides individuals with new rights one of which is the Right to Data Portability. The Right to Data Portability has been further explained by relevant European data protection bodies' guidelines (European Data Protection Board, Article 29 Working Party, Information Commissioner's Office). Article 29 Working Party and Information Commissioner's Office refer to midata initiative in the United Kingdom as an exemplary application of the Right to Data Portability. We investigate whether midata initiative is compliant with the Right to Data Portability and these guidelines as it was claimed by relevant European data protection bodies. In this thesis by using open, axial and selective coding to compare and explain the relationships between midata and these guidelines, we found that while midata is compliant with the Right to Data Portability and these guidelines in some respects, it is also not compliant regarding certain elements. We believe that our findings should provoke and shape revisions of these guidelines as many privacy professionals look at these guidelines to understand and interpret General Data Protection Regulation's Right to Data Portability. This thesis also translates the Right to Data Portability's provisional requirements to action plan steps in the context of data, technology and management. It provides good practice recommendations, scenarios and discussions for project managers and privacy professionals to support decision making and management practice in the application of the Right to Data Portability.

Keywords

General Data Protection Regulation, the right to data portability, data protection, privacy, midata, European Data Protection Board, Article 29 Working Party, Information Commissioner's Office, data governance

KİŞİSEL VERİ TAŞIMA HAKKININ UYGULANMASI: TEKNİK VE İDARİ BIR YAKLAŞIM

ÖZET

Avrupa Birliği'nin Genel Veri Koruma Tüzüğü bireylere "Veri Taşıma Hakkı" adında yeni bir hak tanımaktadır. Avrupa veri koruma otoritelerinin rehberleri(European Data Protection Board, Article 29 Working Party, Information Commissioner's Office) Veri Taşıma Hakkı'nı daha detaylı olarak açıklamaktadır. Article 29 Working Party ve Information Commissioner's Office, Birleşik Krallık'ın geliştirdiği midata girişimine veri taşıma hakkının örnek bir uygulaması sıfatıyla referansta bulunmaktadır. İşbu tez, midata girişiminin Veri Taşıma Hakkı'nın hükümleri ve veri koruma otoritelerinin bu konudaki rehberleri ile uyumlu olup olmadığı değerlendirmektedir. İçerikte açık, eksenel ve seçici işaretleme metodlarıyla midata ve bu rehberler arasındaki ilişki ve uyum incelenmekte ve midata girişiminin Veri Taşıma Hakkı rehberleriyle uyumlu olan ve olmayan öğeleri değerlendirilmektedir. Bulgularımız bu rehberlerin yeniden gözden geçirilmesi gerektiğini göstermektedir. Zira, birçok kişisel verilerin korunması uzmanı bu rehberlere bakarak Genel Veri Koruma Tüzüğü'nün Veri Taşıma Hakkı'nı anlamaya ve yorumlamaya çalışmaktadır. Bu tez aynı zamanda Veri Taşıma Hakkı'nın yasal gereksenimlerini veri, teknoloji ve yönetim perspektifinden aksiyon planı adımlarına çeviremektedir. İşbu tez Veri Taşıma Hakkı'nın uygulanması sırasında kullanılmak üzere, proje yöneticilerin ve kişisel verilerin korunması uzmanlarının karar alma ve yönetim pratiklerine iyi uygulama önerileri, senaryoları ve tartışmaları sağlamaktadır.

Anahtar Sözcükler

Genel Veri Koruma Tüzüğü, veri taşıma hakkı, kişisel verilerin korunması, mahremiyer, midata, European Data Protection Board, Article 29 Working Party, Information Commissioner's Office, veri yönetişimi

ACKNOWLEDGEMENTS

First, I would first like to thank my thesis advisor Assoc. Prof. Dr. Mehmet Nafiz Aydın of the Management Information Systems Faculty at Kadir Has University. He simultaneously allowed this thesis to be my own work, and showed the right direction whenever I needed it.

Prof. Hasan Dağ's and Prof.Salih Bıçakçı's office doors were always open whenever I ran into a trouble spot or had a question about my research or writing.

Finally, I must express my very profound gratitude to my girlfriend Delaney Barth, my mother Nursel Erkmen, father Bülent Erkmen, brother Efe Erkmen, Furkan Çizmeci, Kaan Germirli, Batuhan Ceylan, Güven Kahraman and Murat Savaş Selçuk for providing me with limitless support and showing continuous patience throughout my years of study and through the process of researching and writing this thesis.

This accomplishment would not have been possible without their presence and support in my life. Thank you.

Alp Erkmen

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS/ABBREVIATIONS

DPA The UK's Data Protection Act 1998

EDPB European Data Protection Board

EU European Union

GDPR General Data Protection Regulation

ICO Information Commissioner's Office

ICO Guideline Information Commissioner's Office's Guide to the GDPR

midata midata initiative in the United Kingdom

PCA Personal Current Account

PCA Documents Key industry documents for the PCA midata initiative

RTDP the Right to Data Portability

WP29 Article 29 Working Party

UK United Kingdom

1. INTRODUCTION

Right to Data Portability(RTDP) is the right of the individuals/data subjects that allows them to receive and/or transmit to another data controller the personal data which they have previously provided to a data controller. RTDP's scope requires data controllers that are going to provide data back to data subject or another data controller, as requested by data subject, to be in a structured, commonly used and machine readable format.

It should be noted that RTDP is only available for data subjects when requested data have been obtained by data controller by data subject's consent or for the performance of a contract. Data that have been obtained by relying on other lawful basis for processing personal data, stated under Article 6(1), are outside the scope of RTDP such as where processing is permitted when it is necessary for compliance with a legal obligation.

Moreover, RTDP applies only to data provided to a data controller by data subjects; however, the scope of 'provided to a data controller' should be considered in broad terms. Since if personal data are obtained by observation of data subject's activities (such as tracking individual's website usage history), then this data should be considered as provided by data subject as well.

RTDP aims to allow data subjects to freely make the choice regarding who can use their data, so that data may roam between competing service providers and are not 'locked in' by data controllers.

Most importantly, RTDP is a new right introduced by the General Data Protection Regulation (GDPR) and there is not any other rights similar to RTDP under other privacy frameworks around the World except for the brand-new California Consumer Privacy Act of June 2018 which also includes a kind of right to data portability, however, one which does not mandate that organisations build direct personal data transfer capabilities to other organisations and only includes users' right to download personal data(Wang, Y., & Shah, A., 2018). Therefore, data privacy professionals need

clarification on how to apply this right as there are many questions about how to implement RTDP effectively, especially considering related technical challenges (BS, 2018).

Both Article 29 Working Party(WP29) and Information Commissioner's Office(ICO) refer to midata initiative in the United Kingdom(UK) as an application of RTDP (Article 29 Working Party, 2017; Information Commissioner's Office, n.d). We believe it is critical for practitioners to analyze exemplary applications of RTDP so that they can understand what is considered as compliant with RTDP under GDPR. In our thesis we first aim to examine whether midata is actually compliant with RTDP as the WP29 and ICO suggests, by analyzing RTDP provisions, relevant WP29, ICO and midata documents and comparing our findings. We believe our findings are substantial for understanding WP29 and ICO's guidelines, hence Right to Data Portability's application from a technical and managerial perspective.

Furthermore, ensuring compliance is a continous process required by the GDPR. While organisations may interpret their responsibilities differently, planning practices and processes for compliance starting from the design stage will dramatically reduce an organisation's legal and reputational risk for non-compliance. Therefore, it is critical for RTDP project managers and privacy professionals to have a technical and managerial guideline for RTDP's application they can refer to, which we have prepared for this thesis.

1.1 Methodology

We used open, axial and selective coding to compare and explain the relationship between PCA midata documents and WP29 and ICO's guidelines (Gallicano, 2018).

First, we scanned through PCA midata documents, WP29 and ICO's guidelines and created tentative labels for provisions and phrases in these documents. These labels were created just based on the meaning we extracted from the wording (Elo and Kyngäs, 2008). Secondly, we used axial coding to identify the relationship among the tentative labels, which we have obtained using open coding, under the name

comparison subject (Kolb, 2012). Finally, we have grouped the relationships, which we have identified among PCA midata documents and WP29 and ICO's guidelines, as compatible and incompatible elements (Mills, Durepos and Wiebe, 2010).

Relevant provisions and phrases grouped according to their compatibility and relationship with one another without their tentative labels can be seen under Discussions with the title Table 4.1 Open Coding Source Table.

After we have determined elements of RTDP and examined the only official exemplary application of RTDP, which is midata, we decided to use our findings and technical and managerial issues revolving around these findings to show opportunities, problems and best practices regarding the Right to Data Portability for data controllers, who may misunderstand or misinterpret legal requirements of RTDP which directly effects any RTDP implementation effort.

RTDP requires important changes to data governance for those organisations that choose to comply with GDPR, its potential benefits must be known to the managers running RTDP projects so they may involve stakeholders to support its successful application. Being unable to involve relevant stakeholders would result in RTDP projects' failure. Therefore, in our thesis, being a guideline for the managers of RTDP projects, we have included and discussed potential uses of RTDP to give managers much needed tools for involving stakeholders.

We also wanted to include a common barriers list and disccusion for the realization of RTDP's implementation and wide spread adaptability. We listed these shortcomings and obstacles for a successful RTDP application as they should be known by RTDP project managers and privacy professionals so that any foreseeable trouble may be resolved, avoided or mitigated.

Lastly, we have aggregated and proposed good practice recommendations for planning, design and implementation of RTDP in an organisation.

1.2 Roles

For the purpose of easily explaining this comparison we would like to state how roles correspond to one another:

- Data controller and data subject are roles that exist in current (GDPR) and previous European data privacy legislation ("Guide to the General Data Protection Regulation", 2017). Data controller refers to the natural or legal person that determines the purposes and means of the processing of personal data (ibid.). Data subject is the natural person which is identified or identifiable through his/her 'personal data' (ibid.).
- As the account provider is the data controller which determines the purposes and means of the processing of personal data of account holders, data controller that answers a data portability request corresponds to the account provider for the PCA midata initiative ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2018);
- As the comparison providers determine the purposes and means of the processing of personal data of account holders after they receive personal data, "receiving" data controllers correspond to the comparison providers for the PCA midata initiative ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2018).
- "Data subject", correspond to the user/account holder/consumer ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2018).

Table 1.1 The Right to Data Portability and midata Roles Table

Comparison Group	**Comparison Subject**	**Article 29 Data Protection Working Party, WP 242 rev.01, "Guidelines On The Right To Data Portability"**	**Information Commissioner's Office, The Guide to the GDPR**	**"Voluntary code of practice", "Voluntary code of practice – consumer summary", "midata file content standard"**
Roles	Personal data owner	Data subject/Individual/User	Data subject	User/Customer/ Account Holder
	Data controller which provides personal data back to personal data owner as per his/her request	Data controller that answers a data portability request	"Receiving" data controller	Account provider
	Data controller receiving personal data	Data controller that answers a data portability request	"Receiving" data controller	Comparison provider

2. PRINCIPLES AND REQUIREMENTS OF THE RIGHT TO DATA PORTABILITY AND MIDATA

2.1 The Right To Data Portability Requirements

On the 25th of May 2018, GDPR's Article 20, with its entry into force, introduced RTDP which aims to increase the informational self-determination of data subjects in European Union (Fialová, 2018). Although RTDP is considered a single 'right' by the way it is addressed linguistically, it is actually comprised of three separate rights which can be listed as follows (Swire and Lagos, 2013):

- Data subject's right to receive data, which they have provided, from a data controller (original data controller);
- Data subject's right to transmit above mentioned data to another data controller (receiving data controller);
- Data subject's right to request transmission of above mentioned data directly from original data controller to receiving data controller. This right can only be exercised when it is technically feasible for original data controller to conduct such direct transmission.

All of the separate rights mentioned above (under RTDP) are only available for data that have been obtained with data subject's consent or when it is necessary for the performance of a contract (De Hert et al., 2018).

Furthermore, Article 20 requires data controllers to provide data, requested under RTDP, to be in a structured, commonly used and machine readable format.
RTDP allows individuals to move their data out of the initial data controller's database thus preventing lock-in of data ("The Case Against Data Lock-In", 2018).

While WP29 is replaced by European Data Protection Board (EDPB), EDPB endorses WP29's "Guidelines on the Right to Data Portability under Regulation 2016/679, WP242 rev.01" (WP Guideline). Therefore it is crucial for data privacy professionals to understand how WP29 interprets RTDP as it is currently the only RTDP guideline accepted or acknowledged by EDPB, the independent European body, which

contributes to the consistent application of data protection rules throughout the European Union(EU), and promotes cooperation between the EU's data protection authorities.

WP Guideline states certain elements must exist for compliance with GDPR's RTDP:

- GDPR's Article 5 stipulates that data controllers must ensure accuracy of personal data they hold and WP Guideline states that this mandate for data accuracy extends to data which original data controller provides to data subject or receiving data controller within the context of RTDP (Article 29 Working Party, 2017).
- WP Guideline suggests original data controller must use industry or given context standards while providing data in the context of RTDP; in case there are no such standards, WP Guideline suggests the utilization of commonly used open formats (such as XML, CSV, JSON) (Article 29 Working Party, 2017).
- Data subjects should be informed about security risks before exercising their right to receive or transfer data in the context of RTDP according WP Guideline (Article 29 Working Party, 2017).
- RTDP's availability should be communicated to data subjects while original data controller obtains personal data (Article 29 Working Party, 2017).
- Receiving data controller is responsible for obtaining data that is relevant and not excessive. In other words, receiving data controller is responsible for data minimization instead of original data controller (Article 29 Working Party, 2017).
- Original data controller should communicate RTDP capabilities to data subject when data subject wants to close an account managed by original data controller (Article 29 Working Party, 2017).

However, application of these idealistic requirements stated under WP Guideline cannot be undermined to a singular method or strategy as there are various data handling and transfer capabilities available to data controllers ("Interoperability and Portability for Cloud Computing: A Guide Version 2.0", 2017).

Privacy professionals are challenged by implementing these requirements in real-world as there are not any currently working or tested models available for showcase of RTDP's application (Bozdag, 2018).

2.2 Article 29 Working Party & Information Commissioner's Office and their Guidelines

WP29 was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy(European Union, 1995). Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC (European Union, 1995; European Union, 2002). One of which is, providing guidelines to the public on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community. Although, The European Data Protection Board (EDPB) will replace the WP29 as of 25 May 2018, WP29 has published two versions of the guidelines on RTDP in line with its responsibilities ("Guidelines on the right to 'data portability'", 2017). The first version of the guidelines on RTDP was adopted on 13 December 2016 (ibid.). The revised version (WP Guideline) has been adopted on 5 April 2017 (ibid.). For the purposes of this thesis we have examined revised WP Guideline which is corrected compared to its first version. Moreover, during its first plenary meeting the European Data Protection Board endorsed the GDPR related WP Guidelines including revised version of the guideline on RTDP.

Information Commissioner's Office (ICO) is the independent regulatory office of the United Kingdom with the Information Commissioner being appointed by the Crown, it also provides guidelines regarding matters relating to the protection of persons with regard to the processing of personal data and privacy ("Who we are", 2018). ICO has published on its site "Guide to the General Data Protection Regulation"(ICO Guideline), ICO Guideline's raison d'etre is stated as "explaining the provisions of the GDPR to help organisations comply with its requirements", while its audience is determined as "for those who have day-to-day responsibility for data protection", meaning data privacy professionals ("Guide to the General Data Protection Regulation", 2017). RTDP has been included in the ICO Guideline to further clarify how this new right should be interpreted by data privacy professionals (ibid.).

WP Guideline and ICO Guideline both aim to clarify RTDP by providing further explanation on elements of data portability, when does data portability apply and how should data portability be provided. Various scenarios are provided among these explanations; on the other hand, midata is the only application of RTDP referred to by both documents (Article 29 Working Party, 2017; "Guide to the General Data Protection Regulation", 2017).

2.3 midata

midata started out as a voluntary arrangement covering regulated sectors, with the intent of providing consumers better choices and providing a new platform for business innovation("midata company briefing pack", 2012). Focused on providing price comparisons for customers to boost competition, midata requires participating companies to give consumers access to their data in a machine-readable and reusable format. Since midata initiative is a voluntary scheme, none of the businesses are forced in to participating ("Example applications of the midata programme", 2012). Although, midata started out as an ambitious initiative with 26 companies (including companies such as British Gas, MasterCard and Google) publicly announcing their support for the government plan, most of these companies haven't taken any part in the implementation of this initiative ("midata project plan for compulsory customer data", 2012).

midata is currently synonymous with its application in the banking and energy sectors due to its limited practice outside of these sectors ("Example applications of the midata programme", 2012). Moreover, there is not a voluntary code of practice or a similar document available for a consistent application of midata besides the midata initiative for personal current accounts. Furthermore, while giving midata as an example, WP Guideline hyperlinked the official page for midata initiative for personal current accounts (Article 29 Working Party, 2017). Therefore, we will decode midata's application for personal current accounts to determine whether midata is actually compliant with the GDPR, WP Guideline and ICO Guideline, and if so what lessons could be taken for RTDP's real world applications.

2.4 midata For Personal Current Accounts

midata account scheme allows consumers to download their personal consumption and transaction history for their personal current accounts ('PCA') from their account providers, which can then be uploaded to price comparison sites to reveal which account providers offer a better deal ("midata Personal Current Account Comparisons Industry Code of Practice", 2015). PCA midata initiative also aims to provide consumers a better understanding of their spending habits ("midata For Personal Current Accounts", 2015). It should also be noted that PCA midata files can provide a detailed picture of an individual's personal life and thus should be dealt with utmost care for its security and privacy ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2015). Therefore, PCA midata file downloads are available via secure online banking channels ("midata For Personal Current Accounts", 2015).

http://www.pcamidata.co.uk hosts the key industry documents for the PCA midata initiative ("midata For Personal Current Accounts", 2015). "Voluntary code of practice" sets out the best practice for account providers and comparison providers that wish to participate ("midata Personal Current Account Comparison Voluntary", 2015). "Voluntary code of practice – consumer summary" is an overview of the voluntary code of practice specifically aiming consumers ("midata Personal Current Account Comparison Voluntary", 2015). "midata file content standard" standard sets the content and format that account providers should use in their midata files ("midata minimum standard", 2015). These documents (hereinafter together referred to as "PCA documents") are prepared to ensure PCA midata initiative's application is consistent and the account holders' privacy and security are protected.

PCA documents have been agreed by account providers and comparison providers participating in the PCA midata initiative, in consultation with the UK Government and the British Banker's Association ("midata company briefing pack", 2012). PCA documents are prepared to set best practices for participating parties (account providers and comparison providers) and are not law. As PCA documents are voluntary industry codes, their application is not overseen by any regulatory authority.

3. THE RIGHT TO DATA PORTABILITY VS MIDATA

The UK Government took UK's Data Protection Act 1998 (DPA) into great consideration every step of the midata initiative as can be seen from Privacy Impact Assessment Report prepared by the Department for Business Innovation & Skills ("midata Privacy Impact Assessment Report", 2014). However, it should be noted that the DPA is based on GDPR's predecessor Directive 95/46/EC and has no rights like RTDP within its context.

3.1 Compatible Elements

3.1.1 Accuracy of data to be provided

WP Guideline states that data controllers answering a data portability request do not have an obligation to check and verify data's quality before transmission; it is also noted that all data should already be accurate, and up to date, according to the "Principles relating to processing of personal data" stated under Article 5 of the GDPR (Article 29 Working Party, 2017).

Account providers are required to employ best endeavours to ensure the accuracy of midata files according to the PCA documents ("midata minimum standard", 2015).

3.1.2 Utilizing commonly used open format

WP Guideline suggests, where no formats are in common use for a given industry or given context, data controllers answering a data portability request should provide personal data using commonly used open formats such as XML, JSON, CSV (Article 29 Working Party, 2017).

XML, JSON, CSV are also given as an example in the ICO Guideline as examples of structured, commonly used and machine-readable formats that are appropriate for data portability ("Guide to the General Data Protection Regulation", 2017).

CSV is the format of the PCA midata files that account providers should make available according to the "midata minimum standard" document ("midata minimum standard", 2015).

3.1.3 Informing users/data subjects about security risks

WP Guideline and ICO Guideline draw attention to the fact that by retrieving personal data to their own systems, data subjects increase security risks (Article 29 Working Party, 2017; "Guide to the General Data Protection Regulation", 2017). While it is noted that data subjects are responsible for taking the measures against cyber risks in their own systems, it is also stated data controllers should warn data subjects regarding such risks so that subjects may take the necessary steps to protect the data which they will receive (ibid.).

Account providers are required to provide consumers with a description of risks that could arise in accessing their current account information as stated by PCA documents ("midata minimum standard", 2015).

Table 3.1 Compatible Elements Table

Comparison Group	**Comparison Subject**	**Article 29 Data Protection Working Party, WP 242 rev.01, "Guidelines On The Right To Data Portability"**	**Information Commissioner's Office, The Guide to the GDPR**	**"Voluntary code of practice", "Voluntary code of practice – consumer summary", "midata file content standard"**
Compatible elements	Accuracy of data to be provided	• No obligation regarding data quality verification • Data accuracy required because of GDPR's main principles	• No obligation regarding data quality verification • Data accuracy required as a result of GDPR's main principles	• Best endeavours for ensuring data accuracy
	Utilizing commonly used open format	• Encouragement of providing data in commonly used open formats • XML, JSON, CSV as given examples of commonly used open formats	• Encouragement of providing data in commonly used open formats • XML, JSON, CSV as given examples of commonly used open formats	• CSV format as the set standard for PCA midata files
	Informing	• Information	• Information	• Account

	users/data subjects about security risks	regarding data subject's own system possibly being less secure than data controller's systems • Data controller's duty to make data controller aware of security risks with personally retrieving data	regarding data subject's own system possibly being less secure than data controller's systems • Data controller's duty to make data controller aware of security risks with personally retrieving data	provider's duty to inform users about the risks that could arise from accessing data

3.2 Incompatible Elements

3.2.1 Time element of informing users/data subjects

WP Guideline and ICO Guideline explains that in order to comply with the new RTDP, data controllers are required to inform data subjects regarding the existence of RTDP "at the time where personal data are obtained" (Article 29 Working Party, 2017; "Guide to the General Data Protection Regulation", 2017).

Account providers are required to make the PCA midata service easy to find ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2015).

3.2.2 Distribution of roles for data minimization

WP Guideline, further explains that the "receiving" data controller is responsible for ensuring that the data provided for RTDP are relevant and not excessive with the purposes of the new data processing which the "receiving" data controller will handle (Article 29 Working Party, 2017). This is further explained in the WP Guideline with an example:

"Similarly, where a data subject requests the transmission of details of his or her bank transactions to a service that assists in managing his or her budget, the receiving data controller does not need to accept all the data, or to retain all the details of the transactions once they have been labelled for the purposes of the new service. In other words, the data accepted and retained should only be that which is necessary and relevant to the service being provided by the receiving data controller."

A PCA midata file is a record of only up to 12 months of transaction history for the customer's PCA ("midata minimum standard", 2015). The records to be provided by the account provider don't go back further than 12 months. The reason such limit has been put on the size of data with element of time is expressed as:

"The data included is intended to provide the minimum necessary to enable informed analysis so as to reduce security risks and help protect the privacy of the account holder and any third parties mentioned in the transaction data" ("midata Personal Current Account Comparisons Industry Code of Practice", 2015).

Account providers, which are participating in the PCA midata initiative, are required to redact or blank out certain information from the actual account records of the consumer while providing PCA midata file downloads, such as the descriptor field of each transaction, and consumer's name, address, sort code or full account number ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2015).

3.2.3 Availability of information to users/data subjects while closing accounts

Working Party recommends in the WP Guideline that data controllers always include information regarding RTDP before data subjects close an account (Article 29 Working Party, 2017). It has been noted that, this will allow data subjects to take a copy of their data for later use before a contract is terminated and, possibly, data is deleted (Ibid.).

PCA midata initiative does not require or suggest account providers to provide any information regarding the PCA midata initiative before any account closure ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2015). Moreover, PCA midata files are only available for open accounts; closed accounts are not in the scope PCA midata initiative, meaning midata is not available for closed accounts ("midata Personal Current Account Comparisons Industry Code of Practice", 2015).

3.2.4 Data receiving and direct transfer availability

GDPR's Article 20(1) provides data subjects with the right to receive the personal data concerning him or her and transmit this personal data to another data controller. According to Article 20(2), a data subject has the right to transfer her personal data directly to another data controller, without receiving it first. Although, such transfer could be rejected by the data controller when it is not technically feasible, WP Guideline provides further clarification on technical feasibility:

'Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data. If technical impediments prohibit direct transmission, the data controller shall explain those

impediments to the data subjects, as his decision will otherwise be similar in its effect to a refusal to take action on a data subject's request (Article 12(4)).' (Article 29 Working Party, 2017).

ICO Guideline states that "Individuals have the right to ask you to transmit their personal data directly to another controller without hindrance. If it is technically feasible, you should do this." ("Guide to the General Data Protection Regulation", 2017). ICO Guideline provides further clarification on what would be considered as hindrance, by explaining hindrance as "any legal, technical or financial obstacles which slow down or prevent the transmission of the personal data to the individual, or to another organisation" (Ibid.). Moreover, ICO Guideline states that data subjects are at greater cyber risk by retrieving their personal data from a service, since data subjects' data storage are more commonly less secure systems than the storage of the data controller's service (Ibid.). ICO Guideline further underlines that data subjects should be made aware of this situation (Ibid.).

On the other hand, PCA documents require account providers to notify consumers regarding the risks that may arise from downloading PCA midata documents ("midata minimum standard", 2015).

Table 3.2 Incompatible Elements Table

Comparison Group	**Comparison Subject**	**Article 29 Data Protection Working Party, WP 242 rev.01, "Guidelines On The Right To Data Portability"**	**Information Commissioner's Office, The Guide to the GDPR**	**"Voluntary code of practice", "Voluntary code of practice – consumer summary", "midata file content standard"**
Incompatible elements	Time element of informing users/data subjects	• Informing data subjects re: RTDP as a part of complying with RTDP • Informing data subjects re: RTDP while obtaining data(time aspect)	• Informing data subjects re: their rights(including RTDP) while collecting data	• Requirement of PCA midata service to be easy to use and find
	Distribution of roles for data minimization	• Receiving data controller's obligation to ensure provided portable data is relevant to new processing activities	• Receiving data controller's obligation to accept or retain data only relevant to new processing activities	• PCA midata file's coverage being limited to 12 months of customer's transaction history • PCA midata file's content

				not comprised of complete data (censored name, address, full account number)
	Availability of information to users/data subjects while closing accounts	• Recommendation re: informing data subjects about RTDP in case of any account closure	*-Data not available-*	• PCA midata downloads not being available for closed accounts
	Data receival and direct transfer availability	• Data subject's right to directly send data to another data controller "without hindrance" • Technical feasibility being the only exception for obligation to provide direct transfer to another data controller	• Data subject's right to directly send data to another data controller "without hindrance" • Technical feasibility being the only exception for obligation to provide direct transfer to another data controller • Need for assessing tehnical	• PCA midata file's download being available through secure online banking channels

			feasibility of a transmission on a request by request basis	

4. DISCUSSIONS

WP Guideline clearly states its understanding regarding the possibility that there might be other specific European or Member State laws in another field that also provide some form of data portability that is different than GDPR's RTDP (Article 29 Working Party, 2017). WP Guideline draws further attention to the need for assessment on a case by case basis, if there is such specific legislation which might correlate with RTDP(Ibid.). However, WP Guideline gives midata initiative, United Kingdom Government's pre-GDPR data portability project, as an exemplary application of RTDP in the footnotes of the content under the subtitle 'A right to transmit personal data from one data controller to another data controller', as follows:

> 'In addition to providing consumer empowerment by preventing 'lock-in', the Right to Data Portability is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the data subject's control (*Footnote 7*)
> (*Footnote 7*) See several experimental applications in Europe, for example MiData in the United Kingdom, MesInfos / SelfData by FING in France' (Ibid.).

First of all, the way midata initative is referred to in the WP Guideline is incorrect. 'MiData' is the abbreviation for Michigan's Integrated Behavior and Learning Support Initiative, which is an initiative of the Michigan State and irrelevant to RTDP ("Michigan's Integrated Behavior and Learning Support Initiative – MIDATA"). UK's midata initiative should have been referred to by its correct name 'midata'.

Furthermore, although it could be argued that the adjective 'experimental' takes out the necessity for these exemplary applications to be 100% compliant with WP Guideline or GDPR, the extent of these applications' compliance with GDPR could have been stated more clearly in the WP Guideline, as it might give public and data protection professionals the wrong idea regarding what can be construed as a compliant application of RTDP.

Likewise, ICO Guideline refers to midata initiative as an exemplary initiative for data portability:

‘Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.’ (“Guide to the General Data Protection Regulation”, 2017).

ICO Guideline’s reference to midata initiative is more straight-forward compared to WP Guideline, as ICO Guideline claims that the UK already offers data portability through midata. On the other hand, Information Commissioner’s response to the Department for Business, Energy and Industrial Strategy call for evidence on implementing midata initiative in the energy sector, it was clearly stated that:

‘Government may consider that the midata provisions, in practical terms, will be short-lived and significantly overlap with the data portability requirements.’ ("The Information Commissioner’s response to the Department for Business, Energy and Industrial Strategy call for evidence on implementing midata in the energy sector", 2017).

It is for certain that Information Commissioner is clearly aware of the possible mismatches of midata initiative and RTDP; however, ICO Guideline’s language suggests no such awareness.

When we examined the relevant documents, we found that there are elements of PCA midata initiative which are compliant with WP Guideline and ICO Guideline. In all relevant documents it is stated that data which are going to be provided to data subjects should be accurate (Article 29 Working Party, 2017; “Guide to the General Data Protection Regulation”, 2017). While commonly used open formats such as XML, JSON, CSV are encouraged to be used by WP Guideline and ICO Guideline, correspondingly PCA midata documents require account providers to provide data in CSV format (Ibid.; “midata Personal Current Account Comparison Voluntary Code Of Practice”, 2015). Lastly, informing data subjects about security risks that could arise

from accessing and retrieving personal data is recommended as a best practice in all relevant documents.

On the other hand, we also found that there were elements of PCA midata documents which did not match with WP Guideline, ICO Guideline and GDPR provisions.

Firstly, informing data subjects regarding RTDP is a requirement of complying with relevant GDPR provisions as stated by WP Guideline and ICO Guideline(Article 29 Working Party, 2017; "Guide to the General Data Protection Regulation", 2017). However, PCA midata documents make no such suggestion and only require PCA midata initiative to be easy to use and find ("midata Personal Current Account Comparisons Industry Code of Practice", 2015). These requirements may seem similar, however, data controllers need to inform data subjects about the RTDP 'at the time where personal data are obtained', while on the other side, account providers are not required to provide any information regarding PCA midata initiative capabilities at any step of data collection. Therefore, PCA midata initiative does not inform data subjects in time according to GDPR and WP Guideline and ICO Guideline provisions; it can be argued that notification requirements for PCA midata initiative volunteers are not compliant with the RTDP notification requirements, with time aspect.

Secondly, WP Guideline and ICO Guideline state that it is 'receiving' data controller's obligation to ensure provided portable data is relevant to new processing activities; whereas, the account provider limits PCA midata file's coverage to 12 months of customer's transaction history (Article 29 Working Party, 2017; "Guide to the General Data Protection Regulation", 2017; "midata minimum standard", 2015). Moreover, PCA midata file content is not comprised of complete data (name, address, full account numbers are censored by the account provider) ("midata Personal Current Account Comparisons Industry Code of Practice", 2015). These limits set for the PCA midata file may seem beneficial to the privacy of the consumer at first; however, RTDP is not only about data minimization as RTDP's main focus is providing data controllers an increased sense of personal data autonomy by making sure that they have more control over their personal data.

PCA midata documents require account providers to minimize data that can be downloaded by the consumer ("midata Personal Current Account Comparison Voluntary Code Of Practice", 2015). PCA midata file holds less data, compared to what account providers have about their customers' PCA, in terms of time period and content. Contrarily, WP Guideline stipulates that the liability for data minimization is on the 'receiving' data controller, since the 'receiving' data controller is responsible for ensuring that data received or retained within the context of RTDP are relevant and not excessive with the purposes of the new data processing(Article 29 Working Party, 2017). WP Guideline and ICO Guideline further clarify how this could be achieved by the 'receiving' data controller by not accepting all data or retaining what is necessary after initial analysis (Ibid.; "Guide to the General Data Protection Regulation", 2017). WP Guideline's purpose for explaining that the liability for data minimization is on the 'receiving' data controller, is to make sure RTDP's application supports the free flow of personal data in the EU and fosters competition between controllers(Article 29 Working Party, 2017). However, by minimizing the data which account providers are going to provide, and therefore not letting this data reach to the consumer or comparison providers, PCA midata initiative sets out a different path than what RTDP aims to achieve as a tool for free flow of data.

Thirdly, WP Guideline recommends that data subjects should be informed about RTDP before any account closure so that they can receive their personal data to use later on(Article 29 Working Party, 2017). PCA midata documents include no recommendation regarding letting data subjects know about PCA midata initiative opportunities (being able to receive data) before they close their accounts. This substantially effects the awareness of data subjects, as closure of accounts is a time which data subject is more than likely to receive his/her personal data. Furthermore, PCA midata documents stipulate that PCA midata documents are not available for closed accounts; whereas, WP Guideline and GDPR provisions make no such distinction, RTDP is available for any data provided to a data controller by data subjects and obtained by data subject's consent or for the performance of a contract, whether this data is a part of closed or open account ("midata Personal Current

Account Comparisons Industry Code of Practice", 2015). In other words, PCA midata initiative limits the data that is available for download with the status of the account (open or closed), RTDP makes no such distinction (ibid.).

Finally, although the cyber risk notification requirements look the same at first glance, there is a substantial difference with RTDP and PCA midata initiative in terms of cyber risk and the decision which could be made by such notification. RTDP allows data subject to download data and have it directly transmitted to a new data controller. Such direct transmission should be provided if it is technically feasible. However, PCA midata initiative requires data subjects to directly download data for it to be transferred to another data controller (comparison provider) and there is no such method for direct transfer ("midata minimum standard", 2015). Direct transfer to 'receiving' data controllers for PCA midata initiative is technically feasible, since downloads are already made through secure banking channels and APIs could be used for giving direct access to 'receiving' data controller such ("CMA Market Investigation into Retail Banking", 2015). PCA midata initiative's options for obtaining data puts the privacy of the individual at greater risk and is not compliant with what GDPR stipulates for RTDP. We believe it is significantly misleading for midata initiative or PCA midata initiative to be referred as an exemplary application of RTDP in the footnotes of the content under the subtitle 'A right to transmit personal data from one data controller to another data controller' of WP Guideline, while PCA midata initiative doesn't offer transmission of personal data from one data controller to another data controller although it is technically feasible through the use of APIs ("CMA Market Investigation into Retail Banking", 2015; Article 29 Working Party, 2017).

Table 4.1 Open Coding Source Table

Comparison Group	**Comparison Subject**	**Article 29 Data Protection Working Party, WP 242 rev.01, "Guidelines On The Right To Data Portability"**	**Information Commissioner 's Office, The Guide to the GDPR**	**"Voluntary code of practice" (VCOP); "Voluntary code of practice – consumer summary" (VCOP-CS); "midata file content standard" (MFCS)**
Roles	Personal data owner	Data subject	Data subject	User(Customer)
	Data controller which provides personal data back to personal data owner as per her request	Data controller that answers a data portability request	"Receiving" data controller	Account provider
	Data controller receiving personal data	Data controller that answers a data portability request	"Receiving" data controller	Comparison provider
Compatible elements	Accuracy of data to be provided	Data controllers answering a data portability	You also need to ensure that you comply	Account providers should employ

		request have no specific obligation to check and verify the quality of the data before transmitting it. Of course, these data should already be accurate, and up to date, according to the principles stated in Art 5(1) of the GDPR.	with the other provisions in the GDPR. For example, whilst there is no specific obligation under the right to data portability to check and verify the quality of the data you transmit, you should already have taken reasonable steps to ensure the accuracy of this data in order to comply with the requirements of the accuracy principle of the GDPR.	best endeavours to ensure the accuracy of midata files.
	Utilizing commonly used open format	"Where no formats are in common use for a given industry or	"Where no specific format is in common use within your industry or	"CSV format"

		given context, data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction.”	sector, you should provide personal data using open formats such as CSV, XML and JSON. You may also find that these formats are the easiest for you to use when answering data portability requests.” “CSV, XML and JSON are three examples of structured, commonly used and machine-readable formats that are appropriate for data portability. However, this does not mean you are obliged to use them. Other formats exist that also	

			meet the requirements of data portability."	
	Informing users/data subjects about security risks	"How to help users in securing the storage of their personal data in their own systems? By retrieving their personal data from an online service, there is always the risk that users may store them in less secured systems than the one provided by the service. The data subject requesting the data is responsible for identifying the right measures in order to secure personal data in his own	"How to help users in securing the storage of their personal data in their own systems? By retrieving their personal data from an online service, there is always also the risk that users may store them in a less secured system than the one provided by the service. The data subject should be made aware of this in order to take steps to protect the information they have received. The data controller	"Before providing customers with their midata file, current account providers should provide customers with a description of risks that could arise in accessing, transmitting and sharing their current account information – see the Data protection and privacy section for details."

		system. However, he should be made aware of this in order to take steps to protect the information he has received. As an example of leading practice data controllers may also recommend appropriate format(s), encryption tools and other security measures to help the data subject in achieving this goal."	could also, as a best practice, recommend appropriate format(s) and encryption measures to help the data subject to achieve this goal."	
Incompatible elements	Time element of informing users/data subjects	"In order to comply with the new right to data portability, data controllers must inform data subjects of the existence of	"Tell people which rights they have in relation to your use of their personal data, e.g. access, rectification,	"Account providers are to make the PCA midata service easy to use and find. "

		the new right to portability. Where the personal data concerned are directly collected from the data subject, this must happen "at the time where personal data are obtained". If the personal data have not been obtained from the data subject, the data controller must provide the information as required by Articles 13(2)(b) and 14(2)(c)."	erasure, restriction, objection, and data portability."	
	Distribution of roles for data minimization	"In addition, a receiving data controller11 is responsible for ensuring that the portable	"In deciding whether to accept and retain personal data, you should consider	"A midata file is a record of up to 12 months of transaction history for the

		data provided are relevant and not excessive with regard to the new data processing."	whether the data is relevant and not excessive in relation to the purposes for which you will process it. You also need to consider whether the data contains any third party information." "As a new controller, you need to ensure that you have an appropriate lawful basis for processing any third party data and that this processing does not adversely affect the rights and freedoms of those third parties. If you have received personal data	customer's PCA." "To protect your personal information, the file won't contain your name, address, sort code or full account number, and information within certain transactions will be blanked out."

			which you have no reason to keep, you should delete it as soon as possible. When you accept and retain data, it becomes your responsibility to ensure that you comply with the requirements of the GDPR."	
	Availability of information to users/data subjects while closing accounts	"In addition, the Working Party recommends that data controllers always include information about the right to data portability before data subjects close any account they may have. This allows users to take	*-Data not available-*	"midata downloads will be available for existing customers with personal current accounts, via secure online banking channels. midata will not be available for closed accounts."

		stock of their personal data, and to easily transmit the data to their own device or to another provider before a contract is terminated."		
	Data receival and direct transfer availability	"Secondly, Article 20(1) provides data subjects with the right to transmit personal data from one data controller to another data controller "without hindrance". Data can also be transmitted directly from one data controller to another on request of the data subject and where it is	"What are the limits when transmitting personal data to another controller? Individuals have the right to ask you to transmit their personal data directly to another controller without hindrance. If it is technically feasible, you should do this. You should consider the technical	"midata downloads will be available for existing customers with personal current accounts, via secure online banking channels. midata will not be available for closed accounts."

		technically feasible (Article 20(2)). In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability5 but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible6 . The GDPR does, however, prohibit controllers from establishing barriers to the transmission.”	feasibility of a transmission on a request by request basis. The right to data portability does not create an obligation for you to adopt or maintain processing systems which are technically compatible with those of other organisations (GDPR Recital 68). However, you should take a reasonable approach, and this should not generally create a barrier to transmission. Without hindrance means that you should not put in place any legal, technical	

			or financial obstacles which slow down or prevent the transmission of the personal data to the individual, or to another organisation. However, there may be legitimate reasons why you cannot undertake the transmission. For example, if the transmission would adversely affect the rights and freedoms of others. It is however your responsibility to justify why these reasons are legitimate and why they are not a	

			‘hindrance’ to the transmission.”	

5. IMPORTANCE OF UNDERSTANDING THE RIGHT TO DATA PORTABILITY'S IMPLICATIONS

Value of big data is clearly understood by companies and organisations, as they have seen unprecedented benefits of using big data for decreasing expenses, finding new innovation avenues, adding revenue and launching new products and services (John Walker, 2014). Companies, who are extracting information and value from big data, use personal data of individuals, as well as non-personal data. However, companies' use of personal data, including within the context of big data, is regulated by data privacy(privacy) laws.

Although, there are privacy laws which should limit the collection and use of personal data, individuals' trust in the companies who are collecting and using personal data is thought-provokingly low. As brought to the attention of public by the European Commission's (EC) Factsheet re: The European Union Data Protection Reform and Big Data, only 24% of Europeans have trust in online businesses such as search engines, social networking sites and e-mail services ("The EU Data Protection Reform and Big Data", 2016).

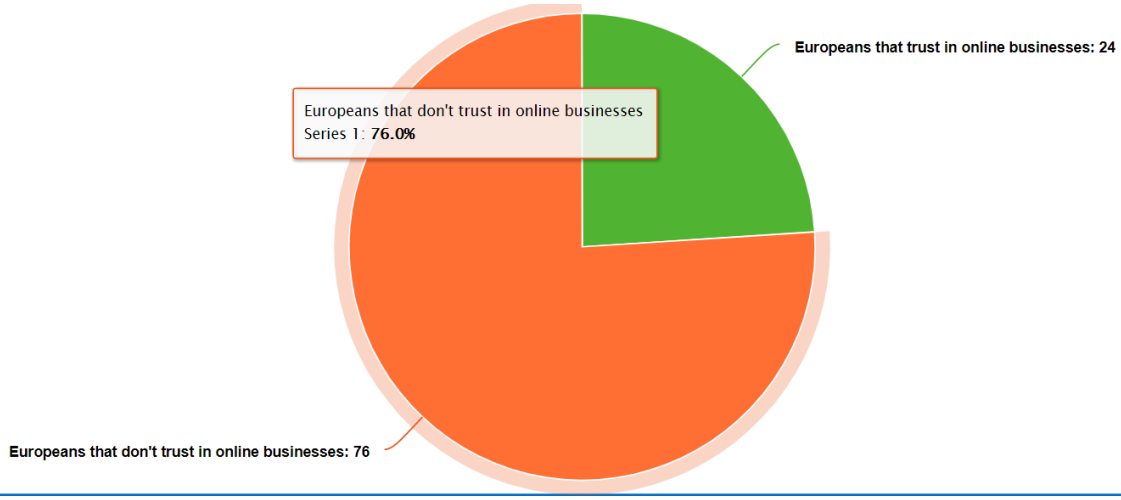


Figure 2.1 Europeans' trust in online businesses

European Union's response to what more could be done against the threats to privacy, while not impeding the ever-innovative data driven economy, is the General Data Protection Regulation, which has taken effect on 25 May 2018 ("Guide to the General Data Protection Regulation", 2017). GDPR is a legislative vanguard with its

introduction of new data privacy rights and unprecedented scope, one of which is the territorial reach. GDPR's territorial scope is unprecedented, as it mandates companies, which are settled outside the EU, to comply with GDPR as well. GDPR applies to companies who are processing personal data of individuals:

- by monitoring their behaviour taking place in the EU; or
- while offering goods and services(whether free or not) to these individuals in the EU.

While drafting the GDPR, European Parliament, Council and Commission(trilogue) took EU citizens' sentiments on data privacy into great consideration (Coppen et al., 2015). European citizens' desires included to have more control over flow of their data. Eurobarometer 431 on Data Protection, the special public opinion survey of the EC, lays out the citizens' sentiments regarding personal data autonomy in the online world: 81% of Europeans feel that they do not have complete control over their personal data online ("Special Eurobarometer 431"). The same survey also shows that: "Two-thirds of respondents who use the Internet (67%) say it is important to them to be able to transfer personal information that was stored and collected by the old provider to the new one when they change online service providers, with 28% saying this is very important, and 39% saying it is fairly important."(Ibid.).

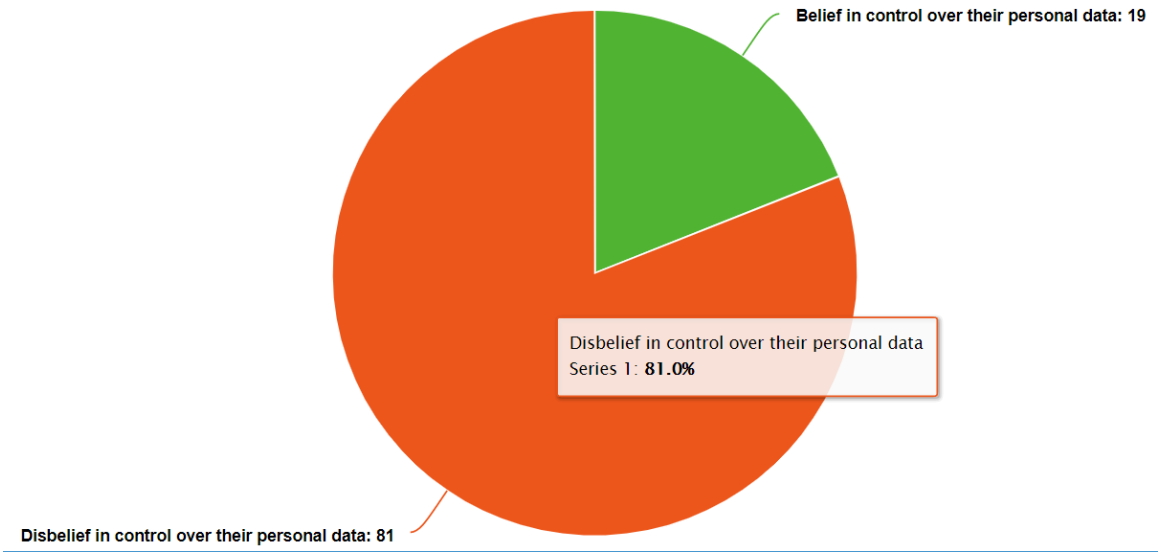


Figure 2.2 Europeans' belief in control over their personal data

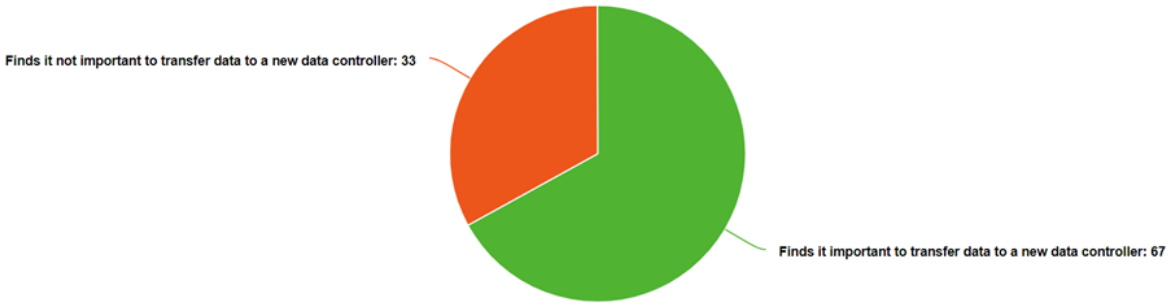


Figure 2.3 Europeans' sentiments regarding importance of data portability

GDPR's potentially most disruptive response to European citizens' need for increased personal data autonomy is "Right to data portability" (RTDP). IAPP-EY Privacy Governance Survey 2017 lists RTDP as the most-difficult compliance obligation in GDPR ("Annual Privacy Governance Report 2017", 2018). RTDP, introduced by the GDPR as a right to receive and transmit certain personal data concerning the individuals, initiates a new chapter in the future of data privacy.

GDPR, with its global applicability, stipulates alarming penalties for infringements regarding RTDP with administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher ("Guide to the General Data Protection Regulation", 2017).

6. POTENTIAL USES OF THE RIGHT TO DATA PORTABILITY FOR CREATING VALUE

The Right to Data Portability forces data controllers to provide data to data subjects and other data controllers whereas there was no such requirement mandated by any regulation before. This compels data controllers to enrich data economy in various aspects.

6.1 Transparency of Data Processing Activities

While the principle of transparency stipulated under GDPR requires companies to be transparent about the personal data they process and store, RTDP forces transparency more concretely since any data provided back to data subjects or other companies will directly reveal processed and stored data which provides transparency (Weiss, 2009).

6.2 Backup Data Convenience

Furthermore, by being able to directly download data, data subjects would be able to backup and have their personal data ready for transfer or further use (Costa & Poullet, 2012). Also, new data backup services can evolve to directly receive data from data controllers as per data subject's request which can be a safer option for data subjects than directly downloading data to their own devices to backup data (Tennison, 2018).

6.3 Service Provider Switching Ease and Competition Stimulation

Although there are similar but narrower scoped legislation provisions forcing data controllers to adapt practices that allow individuals to switch between service providers (e.g. EU Payment Services Directive II for banking sector to share payment data with other service providers if requested), GDPR's RTDP provisions promote service provider switching with a very wide field of application ("Information technology -- Cloud computing -- Overview and vocabulary", 2017). RTDP allows individuals to switch service providers without the worry of losing the value of their account which is created as a result of accumulation of personal data which they have previously provided. For example, if an individual wanted to switch to a new social network because their current one has concerning privacy practices, GDPR stipulates this current social network to provide tools to directly transfer personal data (in the context of RTDP) to a new social network.

In return, this new ease of switching service providers can foster competition in markets (Graef, Husovec & Purtova, 2017). For example, if an individual wanted to transfer their listings (e.g. real estate, second-hand household goods) in a platform to another platform, which they have provided in the first place through strenuous data entry labour, RTDP would streamline the process of data entry labour by mandating the platforms to make this data readily available for other platforms at the request of the individual so that the individual can utilize several platforms all at once by providing data only once (Tennison, 2018). This would in return promote competition by preventing de facto data lockdown ("The Case Against Data Lock-in - ACM Queue", 2018). On the other hand, competition law must be considered and relevant competition law professionals should be consulted while building up any sort of data portability scheme (Geradin & Kuschewsky, 2013).

6.4 Economic Value Added

Another potential value that can arise from RTDP is new complementary services such as data analytics and data management services. As an example, data provided from different service providers can be fed to new data analytics services which in return would give holistic insights that can only be derived through analyzing data provided through multiple resources which can only be avaialable through the implementation of RTDP (opinion et al., 2018). Likewise, data aggregated from multiple services can be managed within a single data management service which in return would make managing multiple service providers all at once significantly easier and plausible.

6.5 Civil Society Benefits

Lastly, data donation can be another potential benefit of RTDP for those individuals who wish to provide data regarding themselves to civil society organisations (Quinn, 2018). Individuals could provide data for research purposes or to be involved in collective action initiations (opinion et al., 2018). Through the widespread adoption of RTDP and massive migration of personal data to civil society organisations for good causes, RTDP can initiate new research avenues or assist in improving the quality of current ones or help communities become organised in unprecedented ways.

7. COMMON BARRIERS FOR THE REALIZATION OF RIGHT TO DATA PORTABILITY'S IMPLEMENTATION AND ADAPTABILITY

7.1 Timeliness of Providing Data

According to Article 12 of GDPR, data controllers have up to a month to respond to RTDP requests ("Guide to the General Data Protection Regulation", 2017). This can deter users from making RTDP requests since nature and need of data processing speed in our world today is instantaneous (Kitchin, 2013). If users cannot have their data instantly available through a RTDP request they cannot utilize the most intended potential benefits of RTDP which we have laid above. Organisations may try to maliciously use this provision to escape or lessen their RTDP requests. However, it should be noted that the relevant provision pre-emptively requires organisations to provide data without undue delay, and one month grace period is only an option for organisations when providing data without undue delay is not possible ("Guide to the General Data Protection Regulation", 2017).

Organisations should make the choice to adopt and develop tools to provide personal data back to their customers without undue delay as stipulated by RTDP not only because it is the ethical way to handle personal data but also because it is required by the GDPR with its alarming penalties for not complying. One month grace period for the realization of RTDP is granted considering small and medium enterprises since their limited financial, human and technology resources may render adoption or creation of RTDP tools within their organisation backbreaking, hence impossible (Article 29 Woking Party, 2017). Creating and providing tools for widespread, financially viable and easy adoption of RTDP is critical for including small and medium enterprises in the ecosystem of RTDP personal data exchange.

7.2 Data Format Differences and Standardisation

WP Guideline suggests that, where there are not any common formats for a specific industry or context, data controllers should provide personal data in open formats such as XML, JSON, CSV(Article 29 Working Party, 2017). However, this does not mean data format standardisation is also a legal requirement stipulated by GDPR, which is a

separate concept (Kaur, Sharma & Kahlon, 2017). This poses a significant risk to successful adoption of RTDP as an organisation can rightfully assume that they may use any commonly used, open format they wish which completely leaves out semantic interoperability issues ("Information technology -- Cloud computing -- Interoperability and portability", 2017). Same data types can be labeled entirely different in a rival organisation.

Without a data format standardisation, all received data within the context of RTDP has to go through syntactic analysis so that the data becomes meaningful for the receiving organisation (Lassila, 1998). However, prior to pondering on running a syntactic analysis for received data, those adopting RTDP projects within an organisation will need to provide data in a preferred or stipulated format for a given context or industry or the data which they provide will not contribute to the adoption and use of RTDP.

7.3 Organisational Policy Differences

Organisational policy differences can defuse the effective widespread adoption of RTDP. There are various decisions that need to be made by the organisation on an ad hoc basis while implementing RTDP solutions in the organisation. Some of these decision points are:

- If the personal data is provided by the data subject or derived from the data subject's provided data.
- If RTDP requesting individual's personal data is entangled with other individuals' personal data. If so, deciding to what extent will such personal data be available for RTDP.
- If it is technically feasible to transfer data or not.
- If the transfer of a certain data would reveal trade secrets.

If the organisation decides that certain data is derived from the data subject's provided data or if RTDP requesting individual's data is inseparably linked to other individuals' personal data or if it is not technically feasible to transfer data or transferring certain data would reveal trade secrets, then relevant RTDP requests can be rejected by the

organisation (Madge, 2018). Simultaneously, these decisions will be made with different approaches by different organisations.

The conditions and considerations that will be effecting these decisions will include appetite for risk, know-how, resources and intentions of the decision making organisation (Khatri & Brown, 2010). Although, the decisions and relevant policies will vary and will be made independently, the collective result will be global. Policy differences, especially organisation policies which have lower standards, can impair the effort for adopting functioning and cooperative RTDP practices ("BS ISO/IEC 19944:2017 Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use", 2018).

7.4 Breach of Security and Trust

Lastly, security should be abstrusely taken into consideration whenever RTDP is implemented since disastrous results can occur for individuals and organisations if security is breached by malicious attackers targeting RTDP channels. Once user trust is impaired through breaches of security while using the RTDP channels, it will not only affect trust in relevant organisations but it will also affect trust in channels that are implemented because of RTDP which they used (Bickmore & Cassell, 2001). This can cause RTDP to receive a mistrusting glare of the public eye. In other words, security breaches are a risk for the successful adoption of RTDP and user trust management.

8. GOOD PRACTICE RECOMMENDATIONS FOR DESIGN AND IMPLEMENTATION OF THE RIGHT TO DATA PORTABILITY IN AN ORGANISATION

Whether an organisation is developing RTDP tools or adopting readily available RTDP tools, in practice organisations will have to conduct a successful project management to implement RTDP solutions. While there are many opportunities with regard to successful implementation of RTDP as we have laid above, in order to conduct a successful RTDP project management there are some aspects which need to be taken into consideration. Regardless of their data processing activities and capabilities, organisations that adapt a successful RTDP program will have the below mutual characteristics.

8.1 Make sure your original intention is carried out

When individuals decide upon tackling difficult projects with predetermined intentions their rate of success dramatically increases (Locke, 1996). RTDP solution implementations can be considered a problematic project management task with various and diverse internal actors that have to act together to decide on various issues in the project implementation stage such as IT Department, Legal or Data Protection Office, Data Governance, Business Units, Communication, 3rd Party Services and Top Management ("Mesinfos Pilot Project Using Self Data", 2018).

Therefore it is very important to determine the scope and goals of the project at the outset of the project for the success of it while communicating with and managing so many individuals coming from different roles.

8.2 Plan resources and positioning channels according to demand

Planning stage of RTDP implementation in an organisation should include these steps:

- Introducing what RTDP is to all actors involved in the project;
- Submitting a list of personal data eligible for RTDP;
- Analyzing the list and confirming these analysis;
- Selecting the data transfer mechanism ("Mesinfos Pilot Project Using Self Data", 2018).

While selecting the data transfer mechanisms the project management team may discover that their resources are insufficient for making all relevant personal data available for transfer through every possible channel (Opsahl & Gebhart, 2018). At this point the team needs to make a decision. This decision should follow the principle of choosing the channels that are most used by the customers/users and ignoring channels where demand is low. By following this principle, RTDP project's implementation will result with maximum amount of benefit through availability.

8.3 Minimise data collection while designing or redesigning your data collection practices

While data minimisation is one of the principles stipulated under GDPR it is also suggested for the RTDP project team to revisit data collection practices of the organisation after the implementation stage (Riechert & Horn, 2018). While analysing the list of eligible data for RTDP, it is good practice to determine excess of listed personal data so that the organisation can put an end to the data collection practices without a legal basis to avoid hefty fines (Ibid.).

8.4 Do not reinvent the wheel – Use available standards

While adopting RTDP in an organisation, using readily available standards would allow significantly cutting costs and reducing time at the implementation stage of RTDP projects ("Cloud Computing Security, Privacy and Forensics: Issues and Challenges Ahead", 2018).

Meanwhile, it is also good practice to be on the lookout for new standards since they are continuously developed and adopted (Kosanke, 2006). After the team has delivered its original goals, regularly revisiting and reconsidering the standards the organisation uses at the RTDP project can allow the organisation to improve its RTDP practices and involvement with the RTDP ecosystems.

Furthermore lack of consistency in standards is an important obstacle that needs to be overcome to successfully implement RTDP on a widespread basis (Chen & Doumeingts, 2003). After all, if there is an available standard that is commonly used it

is only sensible to use it; if there is not an available standards always prioritizing user experience and making things easy for users is the best course of action (Willard et al., 2018).

8.5 Include metadata to support the use of data available through Right to Data Portability

A consequence of efficient and widespread application of RTDP would be the increase of availability, scope and richness of data in an organisation through the migration of individuals' data from different organisations. Importance of metadata and data governance is evident in an organisation which aims to actively use data for decision making and developing new services (Khatri & Brown, 2010).

In order to correctly determine which datasets should be available for RTDP, metadata tags need to be used for entire personal data sets in an organisation (Urquhart et al., 2010). Questions for creating some of the twofold tags (true or false) that can be used for metadata management are shown in Table 7.1 below (Wang & Shah, 2018).

Table 7.1 Metadata Tag Questions and Relevant Parties

Questions	**Relevant party**
- Is data provided by the data subjects (individual)?	• Data Governance • Business Units • Legal and Compliance Departments
- Does data identify individual yet it is derived data(personal data created through the manipulation or analysis of provided data) from "regular" personal data, for example an individual's name revealing predictions about the individual's nationality or religion?	• Data Governance • IT Department • Legal and Compliance Departments
- Can data be used to identify any individual through data management	• Data Governance

practices (e.g. aggregation) or attacks(e.g. SQL injections)?	• IT Department
- Does data direct identify any individual?	• Data Governance • IT Department • Business Units • Legal and Compliance Departments
- Is data anonymous?	• Data Governance • IT Department
- Is data processed based on consent or on a contract?	• Data Governance • Legal and Compliance Departments

Richness and actuality of available metadata will directly affect the results of an organisation's RTDP projects (Rosenbaum, 2010). Furthermore, metadata management will allow tracking those situations where multiple data subjects' data are bundled together and help avoid revealing personal data of those who did not make a RTDP request.

8.6 Construct your RTDP channels for users

Using RTDP tools must be intuitive, meaning they should be simple and straightforward enough for new and unsophisticated users (Robbins, 2016). Moreover, they should be easy to find and RTDP's availability should be notified to users during any account closure and the collection stage of the relevant data. Always include information regarding RTDP before data subjects close an account (Article 29 Working Party, 2017). This will allow individuals to take a copy of their data for later use before a contract is terminated and, possibly, data is deleted.

To put it all together, the data portability should not be built as a quirky tool hidden in the depths of your organisation's online channels known only to privacy enthusiasts.

Figure 8.1 Notification Regarding The Right to Data Portability Opportunities

8.7 Allow users to select which data they would like to transfer or download

It is not the job of the organisation that is answering a RTDP request to minimize the data available for transfer or download (Article 29 Working Party, 2017). It is the receiving organisation's responsibility to not keep data, received through RTDP, which is irrelevant to the legitimate data processing activities they hold.

On the other hand, an organisation that is answering a RTDP request should allow users to select which data they would like to transfer or download whenever they can. In other words limiting the data available for transfer or download at the request of users is a good idea whereas limiting available data for transfer or download due to self-determined organisational decisions is going against the RTDP guidelines and spirit.

8.8 Consider security of data and individuals

While retrieving personal data to their own systems by downloading data available through RTDP, individuals increase security risks (Riechert & Horn, 2018). While it is noted in RTDP Guidelines that individuals are responsible for taking measures against cyber risks in their own systems, it is also stated organisations should warn individuals

regarding such risks so that subjects may take the necessary steps to protect the data which they will receive (Article 29 Working Party, 2017).

However, notifying users about security risks is not limited to the risks which arise from downloading data to their personal systems; a malicious recipient of transferred data can actively use captured data for fraudulent and criminal activities. Therefore, it is also necessary to warn individuals about the risks associated with malicious recipients whenever answering an individual's RTDP request (Riechert & Horn, 2018). It is good practice to include these notifications to users in a clear and concise language before answering their RTDP request.

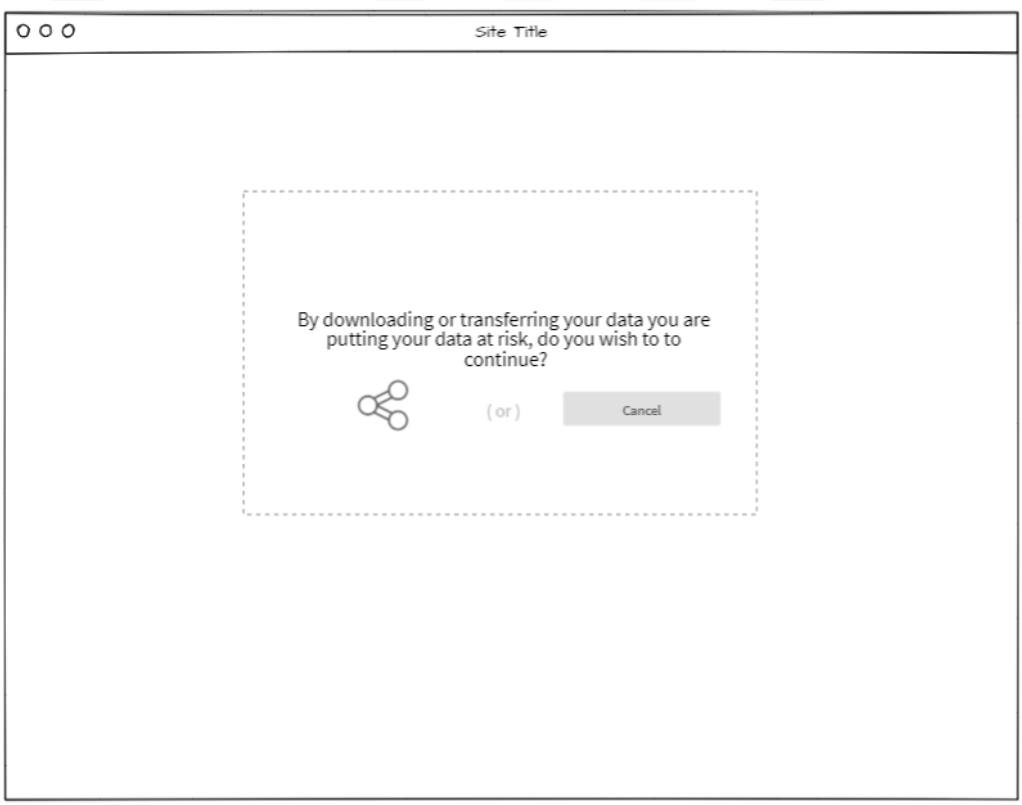


Figure 8.2 Notification Regarding Security Risks of Downloading Data

While informing users about security risks is good practice, security considerations should not be limited to notifications (Willard et al., 2018). End to end encryption protection should be in place during data transmissions between a RTDP request responding organisation and data receiving organisation or the individual making RTDP requests (Saltzer, Reed & Clark, 1984).

Privacy and security-wise very valuable personal data can be the content of the data transmission, therefore it is very important to make sure data transmissions are encrypted as a protection for confidentiality of data. Using a one-time session key which is also encrypted with master keys is an important design concern for the system providing infrastructure for RTDP data transfers (Liu, Cheng, Cao & Jiang, 2013).

Authentication is the answer if you ask how to verify the identity of customers who are making RTDP requests. There are various authentication methods some of which are ("Data Permissions Catalogue – IF", 2018):

- Multi-factor using a generator
- Multi-factor using an object
- Multi-factor using text message
- Secret answer
- One-time access

While implementing integration methods one should also remember to integrate token revocation to the authentication system so that users' authentication identity will be revoked at the end of data transfer (Bender, Kügler, Margraf & Naumann, 2010). It is also important to provide statistics (start and end time of sharing) of data transfers. Furthermore, allowed access time for the users' account should be predetermined and access should be revoked once allowed access time ends ("Data Transfer Project Overview and Fundamentals", 2018). While selecting software from RTDP and API solution vendors, one must ensure their features allow token revocation.

Users also should be notified when a RTDP data transfer happens, for example a push notification can be used to notify users' mobile devices or their mail account can be used to send a notification mail ("Just-in-time consent - Data Permissions Catalogue - IF", 2018). Such notification will help detect unsolicited RTDP data transfers and notify relevant parties to respond to the incident ("Data-responsible Enterprises", 2018). Response may include ceasing any ongoing transfer, and reporting any incident to relevant internal parties, users and authorities. The question of which parties should be

notified is a question that needs to be answered by the Legal and Compliance Departments, make sure these departments are consulted immediately before sending any breach report to relevant parties or making any statements to public. Top Management and Communications department should also be involved with the public statement preparation and release.

Convenience, allocated resources and security are aspects of the system design of RTDP projects which an organisation must balance in order to deliver worthy results. Overall you must always include security and privacy professionals to your design and re-design processes whether they are in-house or consultants providing support for the implementation of Privacy by Design and Security by Design principles to your RTDP project design. Abuse protection and notification mechanisms can be best picked with the guidance of these professionals (“Data Transfer Project Overview and Fundamentals”, 2018).

9. CONCLUSION

WP Guideline and ICO Guideline refer to midata initiative as an exemplary application of RTDP (Article 29 Working Party, 2017; "Guide to the General Data Protection Regulation", 2017). Most importantly, PCA midata initiative is the only quantifiable application of midata initiative so far; furthermore, PCA midata documents are directly hyperlinked in the WP Guideline.

After careful evaluation of PCA midata documents, we have found aspects of PCA midata initiative that were both compatible and incompatible with GDPR's RTDP, WP Guideline and ICO Guideline. Although PCA midata documents are compliant with RTDP, WP Guideline and ICO Guideline in many aspects such as ensuring accuracy of data, encouraging commonly used open formats and informing data subjects about security risks before providing data subjects their data.

There are also elements which we found in PCA midata document that were incompatible with RTDP, WP Guideline and ICO Guideline. WP Guideline and ICO Guideline requirements include informing data subjects regarding RTDP at the time personal data are obtained (where the personal data concerned are directly collected from the data subject), however this is not written under PCA midata documents (Article 29 Working Party, 2017; "Guide to the General Data Protection Regulation", 2017). Similarly, WP Guideline and ICO Guideline require the 'receiving' data controller to apply data minimization principles, whereas PCA midata documents require PCA midata file to be readily minimized before they are given to a data subject (Ibid.; "midata Personal Current Account Comparison Voluntary Code Of Practice", 2015). Moreover, WP Guideline recommends data controllers to provide information to data subjects about RTDP before any account closure, while on the other hand PCA midata documents neither suggest nor require such information to be provided before any account closure (Article 29 Working Party, 2017). Most importantly, while PCA midata initiative only allows data subjects to download data, RTDP requires data controller to provide data subjects the option to choose between a direct retrieval/download by the data subject or a direct transfer to another 'receiving' data controller (Article 29 Working Party, 2017).

Considering PCA midata initiative's incompatible elements with RTDP, WP Guideline and ICO Guideline, it is clear that the way to address midata initiative should have been considered more carefully by the WP29 and ICO before addressing midata initiative as an exemplary application of RTDP in their guidelines. While WP Guideline refers to PCA midata initiative as an experimental application of RTDP, the aspects that are compatible and incompatible could have been examined in detail within WP Guideline (Article 29 Working Party, 2017). ICO Guideline directly states that 'some organisations in the UK already offer data portability through midata', this wording is clearly less noncommittal than WP Guideline's wording which makes ICO Guideline more in need for a change regarding the way midata initiative is addressed ("Guide to the General Data Protection Regulation", 2017).

We believe that this thesis provides guidance regarding how to address exemplary applications of RTDP in relevant guidelines of data protection bodies. We believe that if our findings are not taken into consideration and these guidelines are not revised, data protection professionals can be misled while they seek guidance on the impeccable application of RTDP.

After analyzing RTDP's elements and official exemplary application midata, we have come to realize satisfying RTDP's legal requirements in an organisation must be a collective effort. We have translated these legal requirements to data governance, management and technical action plan discussions. Through this translation we have unraveled various decisions and considerations that need to be evaluated on a case-by-case basis. We have put together these good practice recommendations in logical order for ease of use as a guideline for RTDP project managers and privacy professionals. Moreover, we included scenarios and discussions to help secure stakeholder buy-in for RTDP capabilities adoption in an organisation. We believe discussions in this thesis will be invaluable for professionals who would like to avoid common barriers for the legally compliant realization of RTDP in their organization.

References

Annual Privacy Governance Report 2017. (2018). Retrieved from https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf

Article 29 Working Party. (2017). Guidelines on the right to data portability - Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

Bender, J., Kügler, D., Margraf, M., & Naumann, I. (2010). Privacy-friendly revocation management without unique chip identifiers for the German national ID card. Computer Fraud & Security, 2010(9), 14-17. doi: 10.1016/s1361-3723(10)70122-6

Bickmore, T., & Cassell, J. (2001). Relational agents. Proceedings Of The SIGCHI Conference On Human Factors In Computing Systems - CHI '01. doi: 10.1145/365024.365304

Bozdag, E. (2018). Data Portability Under GDPR: Technical Challenges.

BS ISO/IEC 19944:2017 Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use. (2018). Retrieved from https://shop.bsigroup.com/ProductDetail?pid=000000000030313039

Chen, D., & Doumeingts, G. (2003). European initiatives to develop interoperability of enterprise applications—basic concepts, framework and roadmap. Annual Reviews In Control, 27(2), 153-162. doi: 10.1016/j.arcontrol.2003.09.001

Cloud Computing Security, Privacy and Forensics: Issues and Challenges Ahead. (2018). International Journal Of Recent Trends In Engineering And Research, 4(3), 10-13. doi: 10.23883/ijrter.2018.4083.xwpna

CMA Market Investigation into Retail Banking. (2015). Retrieved from https://assets.publishing.service.gov.uk/media/576410d140f0b66bda00005b/hsbc-response-to-pdr-open-api.pdf

Coppen, R., van Veen, E., Groenewegen, P., Hazes, J., de Jong, J., & Kievit, J. et al. (2015). Will the trilogue on the EU Data Protection Regulation recognise the importance of health research?. The European Journal Of Public Health, 25(5), 757-758. doi: 10.1093/eurpub/ckv149

Costa, L., & Poullet, Y. (2012). Privacy and the regulation of 2012. Computer Law & Security Review, 28(3), 254-262. doi: 10.1016/j.clsr.2012.03.015

Data Permissions Catalogue - IF. (2018). Retrieved from https://catalogue.projectsbyif.com/

Data Transfer Project Overview and Fundamentals. (2018). Retrieved from https://datatransferproject.dev/dtp-overview.pdf

Data-responsible Enterprises. (2018). Retrieved from http://mesinfos.fing.org/wp-content/uploads/2018/03/PrezDataccess_EN_V1.21.pdf

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. Journal Of Advanced Nursing, 62(1), 107-115. doi: 10.1111/j.1365-2648.2007.04569.x

Example applications of the midata programme. (2012). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/34746/12-982-example-applications-of-midata-programme.pdf

Fialová, E. (2018). Data Portability and Informational Self-Determination. Retrieved from https://journals.muni.cz/mujlt/article/view/2645

Gallicano, T. (2018). An example of how to perform open coding, axial coding and selective coding. Retrieved from https://prpost.wordpress.com/2013/07/22/an-example-of-how-to-perform-open-coding-axial-coding-and-selective-coding/

Geradin, D., & Kuschewsky, M. (2013). Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue. SSRN Electronic Journal. doi: 10.2139/ssrn.2216088

Graef, I., Husovec, M., & Purtova, N. (2017). Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. SSRN Electronic Journal. doi: 10.2139/ssrn.3088458

Guide to the General Data Protection Regulation (GDPR). (2017). Retrieved from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Hintze, M. (2018). Viewing the GDPR through a De-Identification Lens: A Tool for Clarification and Compliance.

Information technology -- Cloud computing -- Interoperability and portability. (2017). Retrieved from https://www.iso.org/standard/66639.html

Information technology -- Cloud computing -- Overview and vocabulary. (2017). Retrieved from https://www.iso.org/standard/60544.html

Interoperability and Portability for Cloud Computing: A Guide Version 2.0. (2017). Retrieved from https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf

John Walker, S. (2014). Big Data: A Revolution That Will Transform How We Live, Work, and Think. International Journal Of Advertising, 33(1), 181-183. doi: 10.2501/ija-33-1-181-183

Just-in-time consent - Data Permissions Catalogue - IF. (2018). Retrieved from https://catalogue.projectsbyif.com/patterns/just-in-time-consent

Kaur, K., Sharma, D., & Kahlon, D. (2017). Interoperability and Portability Approaches in Inter-Connected Clouds. ACM Computing Surveys, 50(4), 1-40. doi: 10.1145/3092698

Khatri, V., & Brown, C. (2010). Designing data governance. Communications Of The ACM, 53(1), 148. doi: 10.1145/1629175.1629210

Kitchin, R. (2013). The real-time city? Big data and smart urbanism. Geojournal, 79(1), 1-14. doi: 10.1007/s10708-013-9516-8

Kolb, S. (2012). Grounded Theory and the Constant Comparative Method: Valid Research Strategies for Educators. Journal Of Emerging Trends In Educational Research And Policy Studies.

Kosanke, K. (2006). ISO Standards for Interoperability: a Comparison. Interoperability Of Enterprise Software And Applications, 55-64. doi: 10.1007/1-84628-152-0_6

Lassila, O. (1998). Web metadata: a matter of semantics. IEEE Internet Computing, 2(4), 30-37. doi: 10.1109/4236.707688

Liu, Y., Cheng, C., Cao, J., & Jiang, T. (2013). An Improved Authenticated Group Key Transfer Protocol Based on Secret Sharing. IEEE Transactions On Computers, 62(11), 2335-2336. doi: 10.1109/tc.2012.216

Locke, E. (1996). Motivation through conscious goal setting. Applied And Preventive Psychology, 5(2), 117-124. doi: 10.1016/s0962-1849(96)80005-9

Madge, R. (2018). GDPR: data portability is a false promise – MyData – Medium. Retrieved from https://medium.com/mydata/gdpr-data-portability-is-a-false-promise-af460d35a629

Mesinfos Pilot Project Using Self Data. (2018). Retrieved from http://mesinfos.fing.org/wp-content/uploads/2017/08/mesinfos_pilot_report_2017.pdf

Michigan's Integrated Behavior and Learning Support Initiative - MIDATA. Retrieved from https://webapps.miblsimtss.org/MIData/Account/Login?ReturnUrl=%2FMiData%2F

midata company briefing pack. (2012). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/34747/12-983-midata-company-briefing-pack.pdf

midata for personal current accounts. (2015). Retrieved from http://www.pcamidata.co.uk/

Midata minimum standard. (2015). Retrieved from http://www.pcamidata.co.uk/445505-v2-PCA_midata_-_file_content_standard_-_March_2015-2.pdf

Midata Personal Current Account Comparison Voluntary Code of Practice. (2015). Retrieved from http://www.pcamidata.co.uk/445201-v2-PCA_midata_code_-_consumer_summary_-_March_2015-2.pdf

Midata Personal Current Account Comparisons Industry Code of Practice. (2015). Retrieved from http://www.pcamidata.co.uk/445081-v2-PCA_midata_industry_code_March_2015.pdf

midata Privacy Impact Assessment Report. (2014). Retrieved from http://odrindia.in/tlceodri/wp-content/uploads/2014/03/Midata-Privacy-Impact-Assessment-Report-.pdf

Midata project plan for compulsory customer data. (2012). Retrieved from https://www.bbc.com/news/technology-19331302

Mills, A., Durepos, G., & Wiebe, E. (2010). Coding: Selective Coding. Retrieved from https://methods.sagepub.com/reference/encyc-of-case-study-research/n56.xml

opinion, K., Hardinges, J., Mahmoud, S., Scott, A., Dodds, L., Smith, F., & Beardmore, D. (2018). Will GDPR and data portability support innovation? – The ODI. Retrieved from https://theodi.org/article/will-gdpr-and-data-portability-support-innovation/

Opsahl, K., & Gebhart, G. (2018). What We Mean When We Say "Data Portability." Retrieved from https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability

Quinn, P. (2018). Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?. Global Jurist, 18(2). doi: 10.1515/gj-2018-0021

Riechert, P., & Horn, D. (2018). Retrieved from https://stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/stiftungdatenschutz_abschlussbericht_Hyperlinks_20180124_01_web.pdf

Robbins, B. (2016). Dissecting the Trustworthiness-Trust Link: How Other-Praising Emotions Mediate the Relation between Perceived Trustworthiness and Trust. SSRN Electronic Journal. doi: 10.2139/ssrn.2733984

Rosenbaum, S. (2010). Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access. Health Services Research, 45(5p2), 1442-1455. doi: 10.1111/j.1475-6773.2010.01140.x

Saltzer, J., Reed, D., & Clark, D. (1984). End-to-end arguments in system design. ACM Transactions On Computer Systems, 2(4), 277-288. doi: 10.1145/357401.357402

Special Eurobarometer 431 “Data protection”. (2018). Retrieved from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf

Swire, P., & Lagos, Y. (2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. SSRN Electronic Journal. doi: 10.2139/ssrn.2159157

Tennison, J. (2018). Data portability. Retrieved from https://www.jenitennison.com/2017/12/26/data-portability.html

The Case Against Data Lock-in - ACM Queue. (2018). Retrieved from https://queue.acm.org/detail.cfm?id=1868432

The EU Data Protection Reform and Big Data. (2016). Retrieved from http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41523

The Information Commissioner's response to the Department for Business, Energy and Industrial Strategy call for evidence on implementing Midata in the energy sector. (2017). Retrieved from https://ico.org.uk/media/about-the-ico/consultations/2013714/dbeis-energy-midata-ico-response-20170210.pdf

Urquhart, L., Sailaja, N., & McAuley, D. (2018). Realising the right to data portability for the domestic Internet of things.

Wang, Y., & Shah, A. (2018). Supporting Data Portability in the Cloud Under the GDPR. Retrieved from https://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf

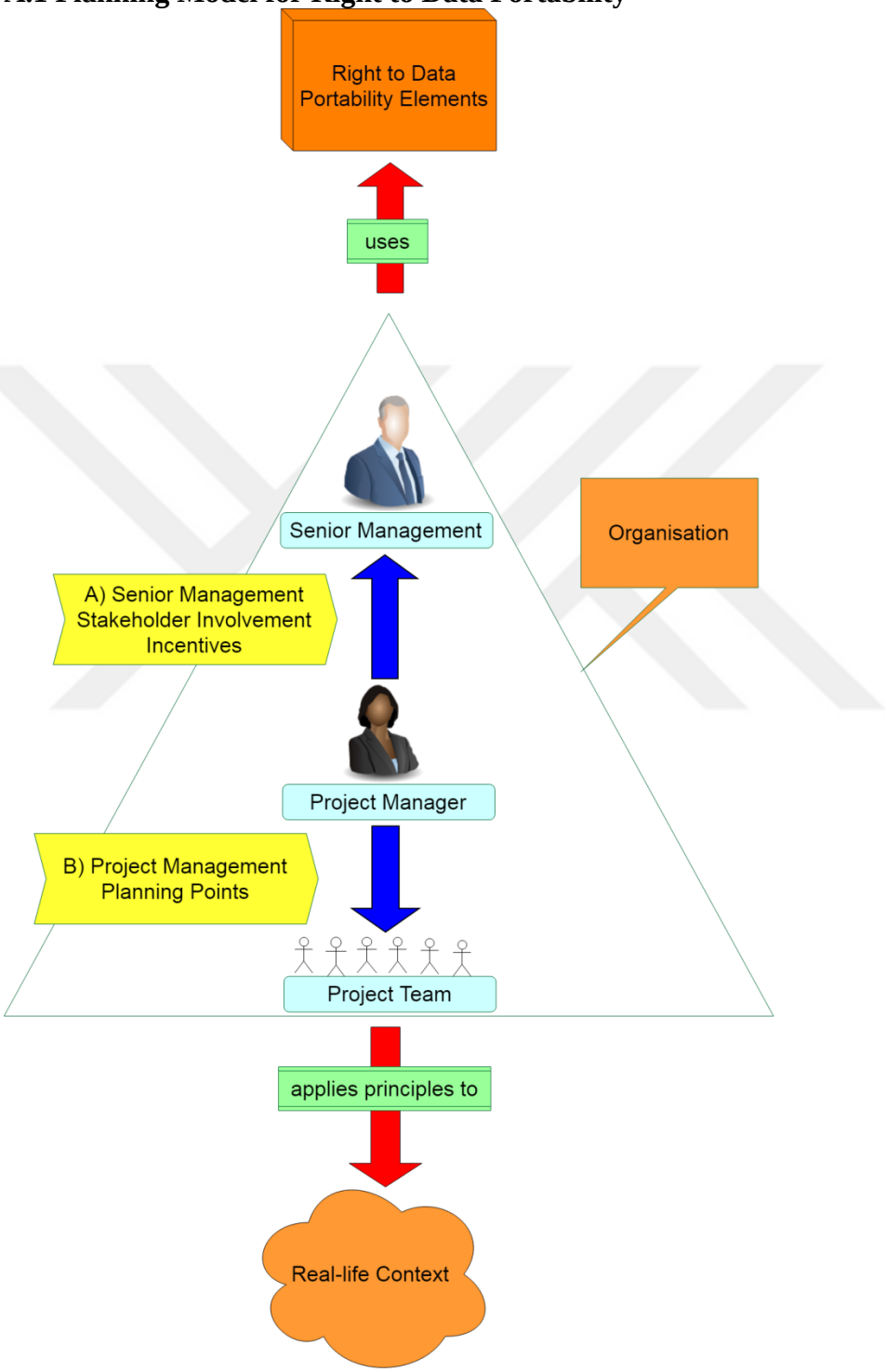
Weiss, S. (2009). Privacy threat model for data portability in social network applications. International Journal Of Information Management, 29(4), 249-254. doi: 10.1016/j.ijinfomgt.2009.03.007

Who we are. (2018). Retrieved from https://ico.org.uk/about-the-ico/who-we-are

Willard, B., Chavez, J., Fair, G., Levine, K., Lange, A., & Dickerson, J. (2018). Data Transfer Project: From Theory to Practice. Retrieved from https://services.google.com/fh/files/blogs/data-transfer-project-google-whitepaper-v4.pdf

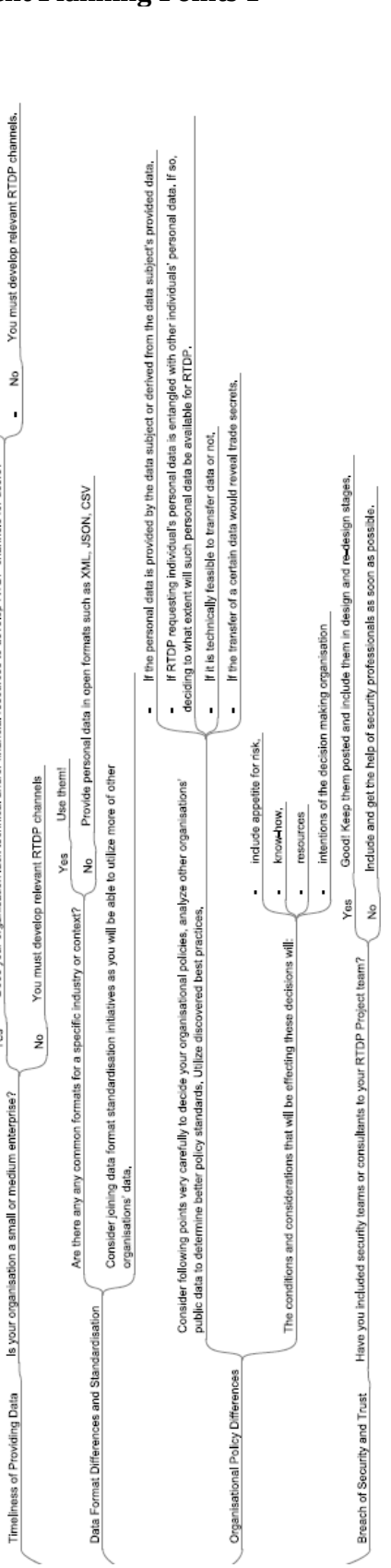
APPENDIX A: RIGHT TO DATA PORTABILITY PROJECT MANAGER TOOLS

A.1 Planning Model for Right to Data Portability

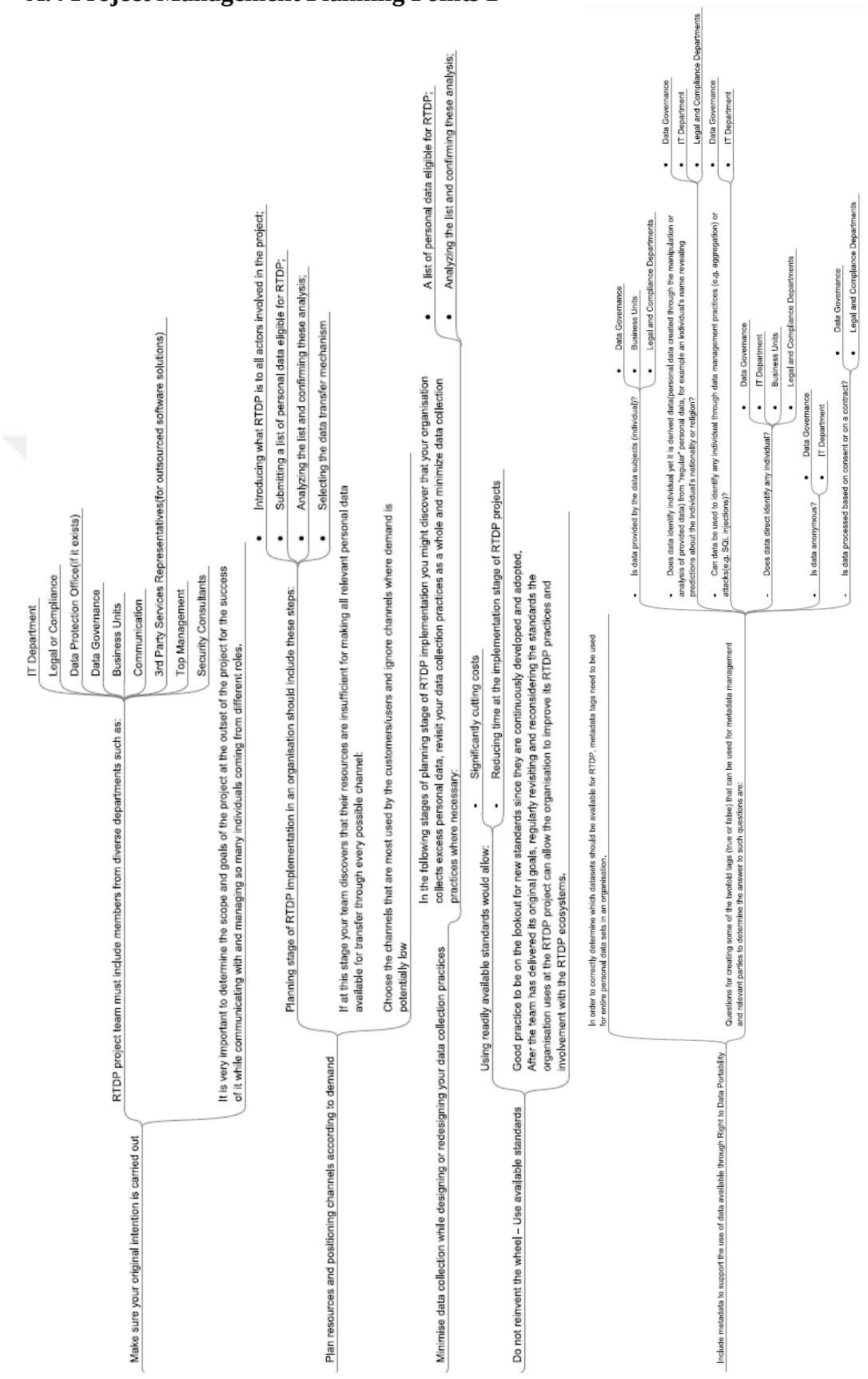


A.2 Senior Management Stakeholder Involvement Incentives

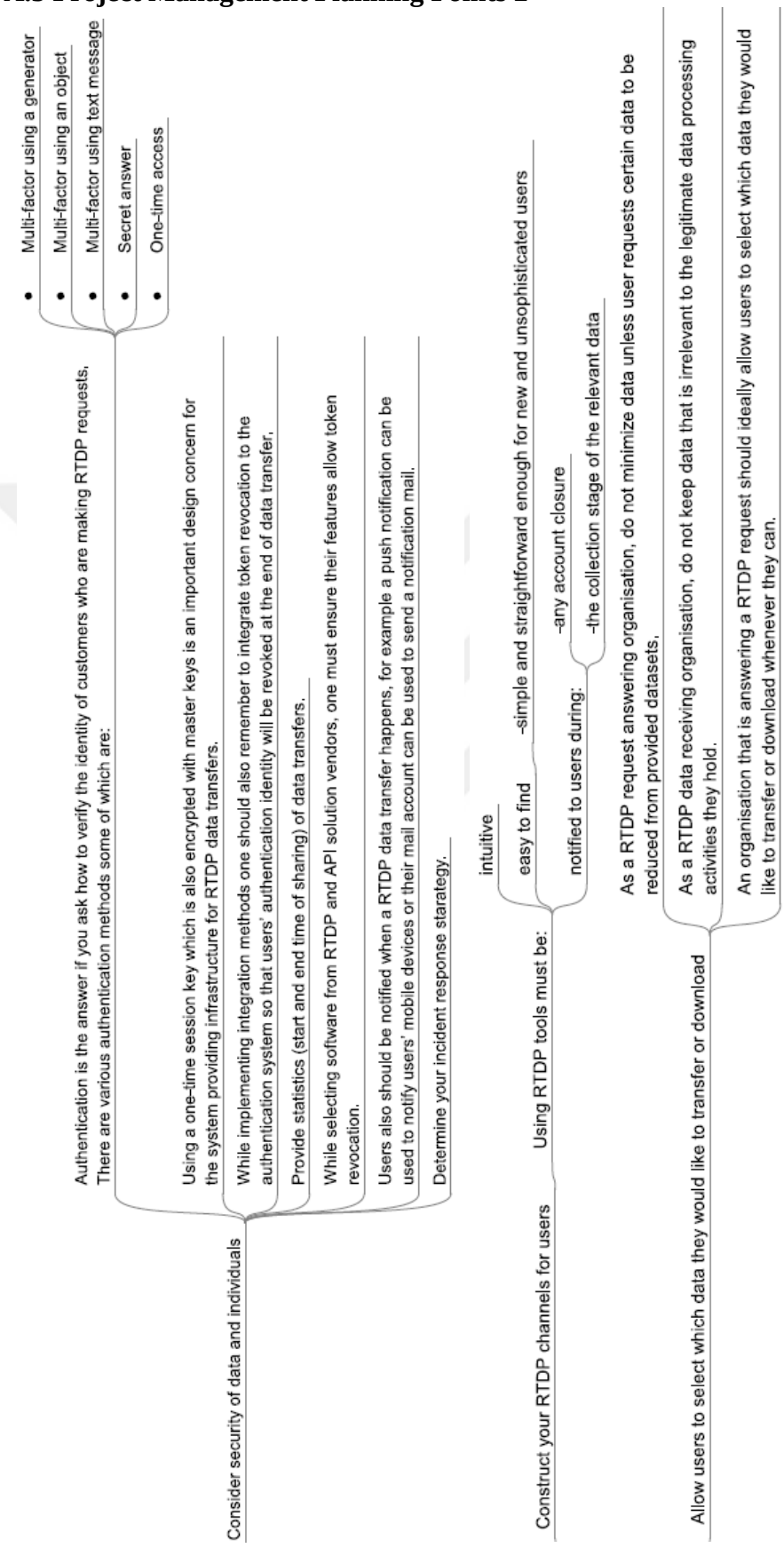
A.3 Project Management Planning Points 1



A.4 Project Management Planning Points 2



A.5 Project Management Planning Points 2



A.5 Right to Data Portability Incident Response Process