A Comparison Between Right to Data Portability and United Kingdom's *midata* Initiative

Alp Erkmen[1*], **Mehmet Nafiz Aydın**[1]

1 Kadir Has University, * Corresponding author, alperkmen@gmail.com

Abstract

European Union's General Data Protection Regulation provides individuals with new rights one of which is "Right to data portability". Right to data portability has been further explained with relevant European data protection bodies' guidelines (European Data Protection Board, Article 29 Working Party, Information Commissioner's Office). Article 29 Working Party(WP) and Information Commissioner's Office(ICO) refer to midata initiative in the United Kingdom(UK) as an application of right to data portability. While technical challenges with right to data portability have been brought forward in other academic papers, we investigate whether midata initiative is compliant with right to data portability and these guidelines as it was claimed by relevant European data protection bodies. In this paper 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 right to data portability and these guidelines in some respects, it is also not compliant regarding time element of informing users/data subjects, distribution of roles for data minimization, availability of information to users/data subjects while closing accounts, data receival and direct transfer availability.

Keywords: General data protection regulation, Right to data portability, Data protection, Privacy, *midata*.

Citation: Erkmen, A., Aydın, M. N. (2018, October) *A Comparison Between Right to Data Portability and United Kingdom's midata Initiative*. Paper presented at the Fifth International Management Information Systems Conference.
Editor: H. Kemal İlter, Ankara Yıldırım Beyazıt University, Turkey
Received: August 19, 2018, **Accepted:** October 18, 2018, **Published:** November 10, 2018

Introduction

Value of big data is clearly understood by companies and organizations, 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 (Bean, 2017). 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(European Commission, 2017).

European Union's (EU) 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 (GDPR), which has taken effect on 25 May 2018 (European Union, 2016). 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. 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", n.d.). 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.".

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 (IAPP-EY, n.d.). 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.

Most importantly, RTDP is a new right introduced by GDPR and there are not any 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 right to data portability (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 (Bozdag, 2018). On the other hand, both Article 29 Working Party(WP) and Information Commissioner's Office(ICO) refer to midata initiative in the United Kingdom(UK) as an application of RTDP (Article 29 Data Protection Working Party, 2017; Information Commissioner's Office, n.d.b). 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 paper we aim to examine whether midata is actually compliant with RTDP as the WP and ICO suggests, by analyzing RTDP provisions, relevant WP, ICO and midata documents and comparing our findings. We believe our findings are substantial for understanding WP and ICO's guidelines and therefore application of RTDP.

What is 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.

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

Article 29 Working Party("WP") 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 WP as of 25 May 2018, WP has published two versions of the guidelines on RTDP in line with its responsibilities. The first version of the guidelines on RTDP was adopted on 13 December 2016. The revised version (WP Guideline) has been adopted on 5 April 2017. For the purposes of this paper 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(Information Commissioner's Office, n.d.c). 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(Information Commissioner's Office, n.d.a). RTDP has been included in the ICO Guideline to further clarify how this new right should be interpreted by data privacy professionals.

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.

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. 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.

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 is currently synonymous with its application in the banking and energy sectors due to its limited practice outside of these sectors. 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. 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.

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. PCA midata initiative also aims to provide consumers a better understanding of their spending habits. 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. Therefore, PCA midata file downloads are available via secure online banking channels.

http://www.pcamidata.co.uk hosts the key industry documents for the PCA midata initiative("Midata for personal current accounts", n.d.). "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", n.d.). "Voluntary code of practice – consumer summary" is an overview of the voluntary code of practice specifically aiming consumers("Midata Personal Current Account Comparison Voluntary", n.d.). "midata file content standard" standard sets the content and format that account providers should use in their midata files ("Midata minimum standard", n.d.). 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. 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.

Right to Data Portability vs midata Comparison

The UK's Data Protection Act 1998(DPA) has been taken into consideration while preparing the PCA documents and standards. Accordingly, The UK Government took 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. 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.

Methodology

We used open, axial and selective coding (Urquhart et al., 2010) to compare and explain the relationship between PCA midata documents and WP, ICO guidelines.

First, we scanned through PCA midata documents, WP and ICO 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.

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.

Finally, we have grouped the relationships, which we have identified among PCA midata documents and WP, ICO guidelines, as compatible and incompatible elements.

Relevant provisions and phrases grouped according to their compatibility and relationship with one another without their tentative labels can be seen in Table 1.

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 (DPA). Data controller refers to the natural or legal person that determines the purposes and means of the processing of personal data. Data subject is the natural person which is identified or identifiable through his/her 'personal data'.
- 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 (referred to as such by WP Guideline and ICO Guideline) corresponds to the account provider for the PCA midata initiative;
- As the comparison providers determines the purposes and means of the processing of personal data of account holders after they receive personal data, "receiving" data controllers (referred to as such by WP Guideline and ICO Guideline) correspond to the comparison providers for the PCA midata initiative.
- "Data subject", correspond to the user/account holder/ consumer.

(see Table 2)

Compatible elements

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.

Account providers are required to employ best endeavours to ensure the accuracy of midata files according to the PCA documents.

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.

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.

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

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. 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.

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.

(see Table 3)

Incompatible elements

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".

Account providers are required to make the PCA midata service easy to find.

Distribution of roles for data minimization

WP Guideline, further explain 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. 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. 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."

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.

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. 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.

PCA midata initiative does not require or suggest account providers to provide any information regarding the PCA midata initiative before any account closure. 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.

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)).'

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.". 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". 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. ICO Guideline further underlines that data subjects should be made aware of this situation.

PCA documents require account providers to notify consumers regarding the risks that may arise from downloading PCA midata documents.

(see Table 4)

Discussions

WP Guideline clearly states its understanding regarding that there might be other specific European or Member State law in another field also providing some form of portability of data that is different than the right to portability stipulated under GDPR. WP Guideline draws further attention to the need for assessment on a case by case basis, if there is such specific legislation which might affect RTDP.

However, WP Guideline gives "midata", United Kingdom Government's pre-GDPR data portability project, which started in 2011 as part of the Government Consumer Empowerment Strategy, 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."

Firstly, the way midata 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. UK's midata should have been referred to by its correct name "midata".

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

Likewise, ICO Guideline refers to midata 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."

ICO Guideline's reference to midata is more straight-forward compared to WP Guideline, as it clearly states that UK already offers data portability through midata.

On the other hand, in the Information Commissioner's response to the Department for Business, Energy and Industrial Strategy call for evidence on implementing Midata 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."

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

When we examined the relevant documents, we found that there are elements of PCA midata initiative which are compliant with WP, ICO guidelines. It is encouraged that data which are going to be provided are accurate in all documents. While commonly used open formats such as XML, JSON, CSV are encouraged to be used by WP and ICO guidelines, PCA documents require account providers to provide data in CSV format in line with WP and ICO guidelines' suggestions. Lastly, informing data subjects about security risks that could arise from accessing and retrieving personal data is recommended as a best practice in all documents.

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

Firstly, informing data subjects regarding RTDP is a requirement of complying with RTDP in accordance with GDPR provisions as stated by WP and ICO guidelines. However, PCA documents make no such suggestion and only require PCA midata service to easy to use and find. These requirements may seem similar, however, for RTDP, where the personal data concerned are directly collected from a data subject, data controllers need to inform data subject 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 service at any step of data collection.

Therefore, PCA midata service does not inform data subjects in time according to the GDPR and WP and ICO guidelines' provisions; it can be argued that notification requirements for PCA midata volunteers aren't compliant with the RTDP notification requirements, with time aspect.

Secondly, WP and ICO guidelines states that it is "receiving" data controller's obligation to ensure provided portable data is relevant to new processing activities; whereas, PCA midata file's coverage is limited to 12 months of customer's transaction history by the account provider, moreover, PCA midata file's content is not comprised of complete data (name, address, full account number are censored by the account provider).

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 but it is also about providing data controllers an increased sense of personal data autonomy by making sure that they have more control over their personal data. WP Guideline explains that the liability for data minimization is on the "receiving" data controller, since the "receiving" data controller is responsible for ensuring that data provided for RTDP are relevant and not excessive with the purposes of the new data processing.

WP and ICO guidelines 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. Asymmetrically, PCA documents require account providers to minimize data that can be downloaded by the consumer. PCA midata files hold less data, compared to what account providers have about their customers' PCA, in terms of time period and content.

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. However, by minimizing the data which account providers are going to provide, without 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. PCA documents make no such recommendation to account providers for information to be included about PCA midata initiative before account holder closes any account. 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 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. 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.

Finally, although the cyber risk notification requirements look the same, 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 since there is a substantial risk

difference between PCA midata initiative and what RTDP provisions require.

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. 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 data. 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 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.

Conclusion

General Data Protection Regulation's(GDPR) right to data portability(RTDP) will force organizations to change their data governance and start new streams of data flow between organizations processing personal data(Horn & Riechert, 2017). Relevant European data protection bodies, such as Article 29 Working Party(WP), Information Commissioner's Office(ICO) and European Data Protection Board, try to bring further clarification on this new right by publishing guidelines. These guidelines aim to provide privacy professionals guidance. These guidelines refer to midata initiative as an exemplary application of RTDP. Most importantly, PCA midata initiative is the only quantifiable application of midata initiative; furthermore, PCA midata documents are directly hyperlinked in the WP's relevant guideline.

After careful evaluation of PCA midata documents, which is the only quantifiable midata initiative for reasons we have laid above, we have found aspects of PCA midata documents that were both compatible and incompatible with RTDP, WP and ICO guidelines. Although accuracy of data that is going to be provided is encouraged to be accurate and CSV is used to provide PCA midata files in a commonly used open format and informing data subjects about security risks is required before providing data subjects their data, there are also elements which we found in PCA midata document that were incompatible with RTDP, WP and ICO guidelines.

A requirement of complying with RTDP is informing data subjects about 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. Similarly, WP and ICO guidelines require the "receiving" data controller to apply data minimization principles, whereas PCA midata documents require PCA midata files to be readily minimized before they are given to a data subject. 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; additionally, PCA midata files are not available for closed accounts while RTDP's applicability does differ according to the accounts' status whether they are closed or open. Most importantly, while PCA midata initiative only allows data subjects to download data, RTDP requires data controller to provide data subjects an option for a download by the data subject or a direct transfer to another "receiving" data controller.

Considering PCA midata initiative's incompatible elements with RTDP, WP and ICO guidelines, it is clear in our opinion that the way to address midata should have been thought more carefully by the WP and ICO before addressing it as an application of RTDP within 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. 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 is addressed.

We believe that this paper could provide further insight for a better way to address application examples in guidelines provided by data privacy institutions.

References

Article 29 Data Protection Working Party. (2017, April 5). Guidelines on the Right to Data Portability. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

Bean, R. (2017, September 20). How Companies Say They're Using Big Data. Retrieved from https://hbr.org/2017/04/how-companies-say-theyre-using-big-data

Bozdag, E. (2018, February 5). Data Portability Under GDPR: Technical Challenges. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3111866

European Commission. (2017, December 21). The EU data protection reform and big data. Retrieved from https://publications.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1/language-en

European Union.Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Union.(1995, October 24). Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Retrieved from http://www.refworld.org/docid/3ddcc1c74.html

European Union.(2002, July 12). Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065

Horn, N., & Riechert, A. (2017, May 12). Practical implementation of the right to data portability – Legal, technical and consumer-related implications. Retrieved from https://stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/studie-datenportabilitaet.pdf

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

Information Commissioner's Office. (n.d.a). Guide to the General Data Protection Regulation (GDPR). Retrieved July 27, 2018, from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Information Commissioner's Office. (n.d.b). Right to data portability. Retrieved from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

Information Commissioner's Office. (n.d.c) Who we are.. Retrieved from https://ico.org.uk/about-the-ico/who-we-are

Midata for personal current accounts. (n.d.). Retrieved July 27, 2018, from http://www.pcamidata.co.uk/

Midata minimum standard. (n.d.). Retrieved July 27, 2018, 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. (n.d.). Retrieved July 27, 2018, 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. (n.d.). Retrieved July 27, 2018, from http://www.pcamidata.co.uk/445081-v2-PCA_midata_industry_code_March_2015.pdf

Special Eurobarometer 431 "Data protection"(Rep.). (n.d.). European Commission. doi:10.2838/552336

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory'back into grounded theory: guidelines for grounded theory studies in information systems. Information systems journal, 20(4), 357-381.

Wang, Y., & Shah, A. (2018, May 25). 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.

Table 1.

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 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.	You also need to ensure that you comply 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.	Account providers should employ 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 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."	"Where no specific format is in common use within your industry or 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."	"CSV format"
	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 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."	"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 could also, as a best practice, recommend appropriate format(s) and encryption measures to help the data subject to achieve this goal."	"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."

Table 1. (cont.)

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)
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 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)."	"Tell people which rights they have in relation to your use of their personal data, e.g. access, rectification, erasure, restriction, objection, and data portability."	"Account providers are to make the PCA midata service easy to use and find. "
	Distribution of roles for data minimization	"In addition, a receiving data controller11 is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing."	"In deciding whether to accept and retain personal data, you should consider 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 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."	"A midata file is a record of up to 12 months of transaction history for the 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."
	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 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 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."
	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 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."	"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 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."	"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."

Table 2.

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	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

Table 3.

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 users/data subjects about security risks	Information 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	Information 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	Account provider's duty to inform users about the risks that could arise from accessing data

Table 4.

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 feasibility of a transmission on a request by request basis	PCA midata file's download being available through secure online banking channels