UiO : Faculty of Law
University of Oslo

Personal Information Management Systems and the GDPR

A review of PIMS as a facilitator for compliance with the GDPR

Candidate number: 8016

Submission deadline: 01.12.2017

Number of words: 17 686

Table of contents

1 Introduction

A personal information management system (PIMS)[1], is a system where people can control their personal data, therein how their data is accessed, collected and used by others.[2] A central feature of the PIMS is the possibility for communication of or withdrawal of consent to any third party.[3] With PIMS the data subject[4] would have a space where the use of their personal data is the focus.

In today's technical world keeping track of one's personal data is becoming increasingly difficult. Data is collected through almost everything we do, both by information given knowingly, as well as through other activities which also produces data; such as credit card use, activity tracking devices and web-browsing.[5] The GDPR provides a ruleset common for all EU and EEA member states. Where the Directive[6] (DPD) was not directly applicable the GDPR is.[7] The rules are strengthened with one common wording applicable to all member states, leaving less room for national interpretation. It provides EU businesses with the same wording applicable for everyone, and should make EU cross boarder data flow easier. This is also positive for data subjects, as they have the same rights no matter where the business is located since the territorial scope of the GDPR goes beyond the EU.[8] In particular, the GDPR is expected to have limiting effect on the way businesses who take advantage of the enormous amount of data available – a part of the concept of big data[9] - get access to and allowance to use this data. This type of data use will often not be compliant with the Regulation, as it sets higher requirements in regards to purpose limitation and consent to name a few. However, this use of data also has several positive aspects; better insight in – for example – crime, criminal behaviour and public health.[10] It allows for businesses to make informed decisions based on large

[1] Personal data stores is another used term, which for the purpose of this paper has no significant difference content wise, the use of PIMS is preferential due to the use of the term "PIMS" in the EDPS Opinion 9/2016. Reference will be made to papers regarding personal data stores, without any difference in meaning being implied.

[2] EDPS Opinion 9/2016 p. 5 paragraph 4.

[3] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015)

[4] GDPR Article 4(1)

[5] World Economic Forum. (2013) p. 7 and 8

[6] Directive 95/46/EC

[7] Article 288 Treaty on the Functioning of the European Union (TFEU).

[8] GDPR Article 3

[9] Laney (2001)

[10] Lepri, Staiano, Sangokoya, Letouzé, Oliver (2017)

quantities of data and algorithms.[11] At the same time, people are becoming more aware of how their data is used and how they can protect it.[12]

The European Data Protection Supervisor (EDPS) states in its opinion on PIMS that the new regulatory framework, the GDPR (Regulation)[13], will facilitate the new reality of human centric control of personal data.[14] And within this, that the new Regulation will open up opportunities for "businesses to develop innovative personal data based services built on mutual trust."[15] That the Regulation sets the foundation for better data security, as well as set the foundation to enforce our security systems.[16] PIMS is then cast as a possible "ideal" business model for such personal data based services by virtue of their technical architecture, data management organisation and trust frameworks.[17]

In order for PIMS to fulfil its potential the EDPS concludes with the need for support in all areas of data services, to help shift the provider centric system, towards a user centric system.[18]

In order for PIMS to take the role suggested by the EDPS, it would ideally be attractive both to the data subjects and the businesses who use the data. This thesis will therefore evaluate whether PIMS is a viable option for the data subjects to manage their rights as given by the GDPR, as well as whether it solves any issues in regards to compliance for the businesses who use the data. Can PIMS be a facilitator of the GDPR?

1.1 Thesis question

The EDPS in its opinion, centres the emergence and possible success of PIMS through the implementation of the GDPR. The thesis will for that reason focus on the GDPR.

The objective for this thesis to evaluate is whether PIMS is able to strengthen the data privacy rights of individuals, facilitating compliance for the controllers, as remaining compliant themselves.

[11] EDPS Opinion 7/2015 p. 7

[12] In recent CJEU case, plaintiff cited the recent Snowden revelations as part of his reasoning; C-362/14, *Schrems v. Data protection Commissioner* paragraph 28

[13] Regulation (EU) 2016/679

[14] EDPS Opinion 9/2016 p. 3

[15] EDPS Opinion 9/2016 p. 3

[16] EDPS Opinion 9/2016 p. 3

[17] EDPS Opinion 9/2016 p. 3

[18] EDPS Opinion 9/2016 p. 14

Is PIMS able to support the data privacy rights of the individuals, and the compliance for the controllers? Will the PIMS themselves be compliant with the GDPR? In particular, how do they support the basic data protection principles under the GDPR, both in relation to the individuals' rights and the abidance of the rules relating to these rights for the controllers? And do they support any of the new data subject rights of the GDPR?[19] And can this support be beneficiary to the controllers as well?

In order to answer the question above, there is also a need to discuss how the PIMS itself will be regulated. Would the PIMS itself be considered a processor or a controller? Would it be able to support the market and relevant businesses when looking at it through the basic principles and key provisions of the GDPR? How much effect will PIMS have from the codes of conduct and certification schemes in the GDPR?

These are the main questions this thesis hopes to answer. The legal backdrop for the future of PIMS within the Regulation is the focus.

The thesis will also review real-life examples of PIMS-like programs in function today, and review the literature in regards to PIMS and the questions raised in this thesis throughout.[20]

1.2 Methodology and scope

The method used to research this paper is doctrinal. It is evaluated on the basis of the GDPR, using the different provisions within the legal text as the starting point for a discussion of PIMS suitability according to relevant provisions. The legal text is further researched mainly through literature, and interpreted in the light of how PIMS operating today is working[21].

The thesis is sectioned into three parts excluding introduction and conclusion. In the introduction the thesis question will be presented, then a presentation of PIMS as a system. The first section will discuss the functioning of PIMS and what PIMS can offer both data subjects and controllers. Then the thesis will review the role of the controller and processor under the GDPR, and where PIMS falls within these. The second part is a review of the basic principles under the GDPR, and how these pertain to PIMS and PIMS functioning. Third section will review the main new provisions within the GDPR as listed by the official GDPR website. The thesis is ended with a conclusion.

[19] Voigt, von dem Bussche (2017), Chapter 5

[20] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015)

[21] EDPS Opinion 9/2016 page 6-8

The scope of the thesis will mostly limit itself to the GDPR as its focus as the thesis garners its questions from the EDPS Opinion[22], which stages the new Regulation as an opportunity for PIMS to come into its full potential. The GDPR will not be gone through in its entirety due to limited word count and the general level of the discussion.

1.3 What is a Personal Information Management System?

In the current system most data is stored at each requesting business or controller.[23] Personal information management systems general idea is to shift the location and control of the data away from the controller, and to the data subject.[24] Many PIMS promise their users they can give the users the control of their data back to them, as seen with Mydex[25], open-PDS/SafeAnswers [26] and Hub of All Things[27]. However, PIMS is also a way for the controllers to get usage of relevant data while still remaining compliant with the GDPR and alleviate some of the burden of compliance[28].

Different PIMS have different technical solutions in regards to how the data is stored and accessed by the data subject and controllers.[29] The two technical systems most relevant is storage of data locally with the data subject on their own device, or a cloud based solution.[30] There are also hybrid options available, where you can store data both locally and cloud based, such as a data storage solution with the Respect Network, which is a personal information management system where you can store data both on your own device or network as well as one of their cloud solutions.[31] PIMS can operate on different legal grounds in relation to the individual user; the most likely option is consent[32] but contract based is also a possibility.[33]

[22] EDPS Opinion 9/2016

[23] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 3

[24] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 3

[25] Mydex CIC. (2010) p. 8

[26] openPDS/SafeAnswers (2017)

[27] Hub of All Things (2017)

[28] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 12

[29] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 20 and 21

[30] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 20

[31] Respect Network FAQ (2017)

[32] See GDPR Article 4(11) and 7

[33] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 17

1.3.1 Technical

Personal information management systems will both cloud based and local storage based need good encryption and technical solutions in order to be both secure and convenient to use. Sufficient encryption of the data, and good decrypting techniques for data sharing is key considerations for PIMS.[34] With cloud based PIMS you get the advantage of physical separation of the data and the decryption key which is held by the user, or by a third party.[35] An example of third party verification is the company BankId, which provides a personal key only the user has access to and acts as a digital signature and access code.[36] "Smart contracts" or "link contracts will likely be a part of most PIMS enterprises as this is an efficient and secure way for the data subject to communicate its will.[37] This is also supportive of the obligation of data protection by design and by default in the GDPR.[38]

1.3.2 Functions for data subjects

PIMS promise several benefits towards it users in regards to data protection and other areas of data use.[39] First and foremost, they place the control over their data with each individual user.[40] They act as a storage unit for personal data, which can include information such as insurance agreements[41] or data on relationships with online stores, which is beneficial today when many contracts are done and stored electronically.[42] As the data becomes more collected as opposed to siloed, the users also get the benefit of making more informed decisions based on their data.[43] The users can control consent or withdrawal of consent, or approval of use of data on contractual grounds towards the controllers from the PIMS.[44] In particular the control of data on contractual grounds is relevant to PIMS, as new technology makes PIMS able to through pre-set conditions or interoperable contracts and send the exact data required for the fulfilment of a service or a contract. This is a core function of the PIMS openPDS/SafeAnswers, which is focused on sending back only the data needed for i.e. an app to provide the promised service.[45] Data transfer is today not necessarily something the user is

[34] EDPS Opinion 9/2016 p. 10 and 11

[35] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 22

[36] BankID (2017)

[37] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 25

[38] GDPR Article 25

[39] Ctrl-Shift. (2014) p. 5

[40] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 3

[41] Such as Bought By Many (2015) which provides insurance opportunities modeled after exact needs from the users, and control the information being sent to the insurance providers.

[42] Mydex CIC. (2010) p. 8

[43] Ctrl-Shift (2014) p. 10

[44] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 16

[45] openPDS/SafeAnswers (2017)

aware the businesses do, but with the new Regulation[46] users can be able to be aware of and control this in their PIMS.[47]

1.3.3 Functions for business

As PIMS is the gate through which the businesses – controllers – get the users data from, PIMS use this as an opportunity for co-operation with businesses by also offering services which benefit the controller further.[48] In some cases, to a large degree and arguably as much as it benefits the users. Some businesses are PIMS who target business and offers compliance solutions at the same time as the users have a portal where they access their data.[49]

Trust towards controllers has suffered in recent years as the possible use of data and revelations of to what extent it is used has awakened the public.[50] PIMS use this as incentive towards businesses for the use of its services; the company Crtl-Shift base some of their marketing on a positive relationship with the user and promise to “help you stay trusted and competitive in the digital economy.”[51] PIMS also functions as a facilitator of maximal use of personal data for the business within the framework of the law, Trust Hub markets itself to utilise the business to “Use personal data to drive decision-making across your organisation.”.[52] Anonymisation and pseudonymisation is one of the techniques PIMS offers to business in order for them to garner full use of data.[53] While these techniques remove or lessen need for compliance with the GDPR, actual anonymisation is hard to achieve. PIMS also offers cost saving benefits, in particular for smaller businesses as they pay to use a part of a system already in place.[54] It is also a means to gain systemised consent to use of data. With the new rules in regards to consent and explicit consent this will most likely be attractive to a lot of businesses.[55]

Some of the providers also argue that you get better quality data, which means better and more precise information garnered from that data.[56]

[46] GDPR Article 45 and 49

[47] EDPS Opinion 9/2016 p. 11

[48] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 11

[49] Such as Ctrl Shift and Trust Hub

[50] Hautala (2016)

[51] Ctrl Shift webpage (2017)

[52] Trust Hub (2016)

[53] Trust Hub markets one of their features as “data masking”, which includes anonymisation and pseudonymisation. (2016)

[54] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 11

[55] GDPR Article 7

[56] Mydex CIC. (2010) p. 11

1.3.4 Championed by the European Commission

In order to evaluate whether a PIMS would be a good solution for a more secure data situation in the Digital Single Market, the Commission commissioned a report from the University of Cambridge[57], about the legal, economic, social and technical feasibility of PIMS as this solution. The report is all in all positive in regards to PIMS being the solution for data security for the future, but raises the important issue of whether the system will be able to acquire enough users both on the business side and on the user side for it to function optimally.[58]

The opinion of the EDPS[59] was also overall positive, but stressed the need for cooperation from business, and especially government and member states, for it to be successful. In addition, well-functioning security measures were listed as important.

From a European Union government standpoint, PIMS seems to have support from both the Cambridge paper and the Opinion of the Data Protection Supervisor.

[57] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015)

[58] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 41 and 42

[59] EDPS Opinion 9/2016

2 Personal Information Management Systems in relation to the GDPR

In order to establish in what cases pursuant to the new Regulation PIMS could simplify or add to the data processing as a positive, there is a need to establish in what way the GDPR will directly affect PIMS; will PIMS be considered a controller or processor? What rules will directly apply to PIMS? Therefore, the question; how do PIMS fit into the GDPR, when considering only the PIMS functions and not the PIMS functions towards a controller or data subject?

2.1 Personal data

For data to fall within the scope of the Regulation, the data has to be "personal". According to GDPR Art. 4(1) personal data is "information relating to an identified or identifiable natural person". If the data relates to an identified natural person, it will fall within the scope. The data will also fall within the scope if the data renders a natural person “identifiable” indirectly, within the reasonable means likely to be used to identify the data subject[60] [61] An identifiable person is a natural person who can be identified through the data directly or indirectly when other identifiable data is present, i.e. “location data”. Location data in particular has proven as a highly identifiable type of data, allowing the controller to identify the data subject on the basis on its movements due to the “uniqueness of human mobility”.[62]

It is sufficient that there is a possibility for identification. Data enabling the controller to identify the data subject when seen with other data sets or alone, makes data personal according to the GDPR Art. 4(1).[63]
The Directive operated with reasonable likeliness of identifiability according to recital 26 and judgment *Patrick Breyer v. Bundesrepublik Deutschland* [64] [65]. This is a relative criterion for identification. The judgment takes a decisive stand as to what is "reasonable means"[66] for a controller to identify a data subject. The plaintiff here, Germany, were seen to be able to with "reasonable means" access the necessary information from Breyers’ ISP, and would be able to

[60] Voigt, von dem Bussche (2017), p. 11

[61] Article 29 Working Party. WP136 p. 15

[62] de Montjoye, Hidalgo, Verleysen, Blondel (2013) p. 4

[63] Voigt, von dem Bussche (2017), p. 12

[64] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* paragraph 42

[65] See also Advocate General's Opinion on case C-582/14

[66] Directive 95/46/EC recital 26

match his IP address at the time with his visit to the site in question.[67] There were hurdles for the online media service provider to do this, but even these were not enough for identifiability to be unlikely.[68] The Court[69] also used the Advocate General's Opinion[70], stating that the means must be reasonable, as opposed to "disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[71] There is reason to interpret the GDPR in the same way since recital 26 also references to a standard of "reasonable".[72] Especially considering the nature of the GDPR, which is stricter on several other sections than was the case with the DPD, such as the rules regarding breach notification[73] which has concrete guidelines to timeframes and how to proceed in the case of a data breach.

As mentioned a main goal for PIMS is to put the data subject in the centre of the data control, and to do this the users store their personal data in the PIMS. PIME will therefore always be able to identify the data subject. Such as Mydex which states: "This is a central, critical departure point. Personal Data Stores are first and foremost a 'person-centric' service".[74] In order for the data subject to have control over their personal data they need to know what that data is, and what rules are connected to different the categories of their data.

PIMS also need access to this data in order to fulfil what they promise their uses. PIMS promise to assist the data subjects in this process, such as the PIMS openPDS/SafeAnswers, stating that for users the current metadata[75] sharing "makes it very hard, if not impossible, for an individual to understand and manage the associated risks", and promise their users that with their product their "metadata to be safely shared and reconciled under the control of the individual."[76] Helping them identify what data is valuable, and how to share it in a way that is comfortable for the user. This data will always be personal data, as this is the market PIMS is servicing.

[67] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* paragraph 48

[68] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* paragraph 47

[69] The EU Court of Justice Second Chamber

[70] Advocate General's Opinion on case C-582/14

[71] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* paragraph 46

[72] Voigt, von dem Bussche (2017), p. 12

[73] GDPR Article 33 and 34

[74] Mydex CIC. (2010) p. 8

[75] «digital information about users' location, phone call logs, or web-searches»: de Montjoye, Shmueli, Wang, Pentland (2014)

[76] de Montjoye1, Shmueli1, Wang , Pentland (2014)

PIMS also offers businesses the opportunity to identify personal data as a part of their promise of compliance with the GDPR, and manage personal data for them; often as a product the controller can offer their users. As is the case with the company Ctrl-Shift, which markets itself to businesses as letting the users have control over their personal data, at the same time as their personal data use remains compliant with the GDPR and as a consequence get new and better information from that data.[77]

PIMS will therefore by nature always process personal data, as that is the whole foundation of their business. They will therefore always fall within the scope of the GDPR as far as the personal data in GDPR Article 4(1) goes.

2.2 PIMS as a controller and processor

2.2.1 Controller

The definition of "controller" has not changed from the DPD to the GDPR.[78] The terminology of "controller" and "processor" and their autonomous interpretation across member states was a focus for the EU, as made clear by the Article 29 Working Party (WP29),[79] the terminology and concept of the controller remains with its meaning intact from the DPD[80]. There has however been made an addition of the concept of joint controllers in the GDPR[81], which was possible also under the Directive[82], but is codified and regulated in regards to informing the data subject of the “arrangement” between the controllers in the GDPR.

In order for PIMS to be subject to controller responsibilities they would therefore need to determine the purpose of the use of the data in some capacity. For some PIMS this will be the case, and for others it will not. It will depend on the PIMS in question and what precise services it offers its users. [83]

To be considered a "controller" one must be a “natural or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of the

[77] Ctrl-Shift (2017)

[78] see the GDPR Article 4(7) and the DPD Article 2(d)

[79] Article 29 Working Party, WP 169 p. 8.

[80] Directive 95/46/EC Article 1(d)

[81] Article 4(7) and Article 26

[82] Directive 95/46/EC Article 2(d)

[83] Case C-131/12 *Google Spain v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* paragraphs 32-41

processing of personal data;”[84]. There are three main components to the definition of a controller, these will be gone through in the following paragraphs.[85]

First; the controller definition applies to a "natural or legal person, public authority, agency or other body". A PIMS would most likely be a legal person or a public body.

Second; the controller determines the purpose "alone or jointly with others". This does not mean that they need to be making the decisions at the same time or at the same stage of the process as others; there can be responsibilities for different steps of the process. Joint controllers are now regulated in the GDPR under Article 26. The responsibility for adherence to the GDPR will be shared, and the Regulation demands the controllers to be clear in areas of responsibility by stating they shall; "in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation"[86]. This should also be reflected to the data subjects.[87] [88] For example; the PIMS *Bought by Many* is a service where the data subject has full control over their data and use it to get tailored insurance products.[89] Here the PIMS get the data directly from the data subjects, but in order to offer the promised insurance services it is the PIMS and not the data subject that carries out the communication with the insurance companies. However, as the insurance is offered through the PIMS, the insurance company in itself is not likely to be viewed as sole controller, as the actual choosing of the suitable insurance product for its users would constitute determining of the “purpose and means of the processing”. [90] Making the PIMS and the insurance company joint controllers.

Third, the controller “determines the purposes and means of the processing of personal data”. The determination of the means and the purposes is guiding as to whether someone is to be viewed as a controller or not, as the actual determination of the purpose for the processing of the personal data will make clear who is actually requesting and wanting to use this data. The third element of the definition can be sectioned in two:1) the determining and 2) the purpose and means, where the determining part weighs heavily.

[84] GDPR Article 4(7)

[85] See also Article 29 Working Party, WP 169 p. 7.

[86] GDPR Article 26(1)

[87] Voigt, von dem Bussche (2017), p. 18-19

[88] GDPR Article 26(2)

[89] Bought by Many (2017)

[90] Case C-131/12 *Google Spain v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* paragraphs 32-41

As specified by the WP29, it is the factual background that decides whether an entity is a controller or not: "The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis."[91] So if the PIMS holds the power to decide that the processing takes place, and how, the PIMS will likely be a controller in those cases, with controller responsibilities.[92] PIMS is a system that will vary greatly from provider to provider, whether the PIMS is a controller will depend on what function is used. A system with no other functions than storing your personal data where the data subject catalogues and decides everything about its data will be closest case to not being viewed as a controller. However, a slight shift in services will be enough to qualify as a controller. Such as the Respect Network, with different products for businesses and users as well as services varying in what the Respect Network does. The Respect Network operates with Software as a Service, where the users' data can be self-hosted; meaning all control of the data and information is with the user giving the Respect Network little opportunity to determine means or purpose of that data unless the user requests it.[93] For these purposes the Respect Network is a processor instead of a controller as they state the cloud is fully controlled by the individual, and the Respect Network would have no way to have any control over the data besides what would be done of a processor. However, they also offer services that help manage the data subjects' communication, which will include decisions from the Respect Network as requested by the data subject.[94] They also offer businesses a solution for their customers, where the business' customer can stream the personal data through the Respect Network. The businesses would get an advantage of the use of a PIMS in that they get data directly from the source. But this will require more determining of the data use from the Respect Network as they offer businesses accurate data as well as secure data.[95] For this type of use the PIMS would most likely be a joint controller as it is part of the decision of processing of the data. This is also the case for the Respect Affinity Network: within the Respect Network using information from the users (who have opted for this) to send ads fitting their profile on behalf of business members without actually giving the profile to the businesses.[96] This will require determining of means and purposes of data on a greater level for the Respect Network.[97] And as the Respect Network here is the only party using the data to connect business and user they will be the sole controller for this data, determining who the user will receive ads from, and who the business will send ads to.

[91] Article 29 Working Party. WP 169 p. 9.

[92] Voigt, von dem Bussche (2017), p. 19

[93] The Respect Network FAQ; question "What is a personal cloud?" (2017)

[94] The Respect Network FAQ; question: "Why should I personally join the Respect Network?" (2017)

[95] The Respect Network FAQ; Why else should my business join? (2017)

[96] The Respect Network FAQ; How does the Respect Affinity Network work? (2017)

[97] The Respect Network FAQ; questions regarding Business (2017)

The third element is as mentioned also an evaluation of the "purpose" and the "means" to the processing. The purpose of the processing limits the use of the data while the means show control over how the data is obtained. Both of these evaluated together gives an indication of how the controller use the data, and whether it is in fact within the definition of “controller”. This is especially important when evaluating PIMS as the means can encompass such decisions as to who the data is shared with, how long the data should be processed and similar.

The controller/processor line is fluid, especially considering for PIMS whose functionality varies to some degree on user preferences. Their function can vary from one click to the next, along with status as processor or controller. However, PIMS potential is the possible use it has for both data subject and businesses to simplify their exchange with each other, and optimise the use of data. Such as the PIMS Mydex[98], which allows you to store your personal data, a part of this is nothing further than the storage of data through Mydex which gives Mydex little opportunity to decide on the purpose of the data use. However, they also offer data management, which include authorising access on behalf of the data subject and forwarding of data to requestees where only the PIMS can connect the two.[99] These examples would require the PIMS to determine the means and purpose of how the data subjects’ data is used, and make compliance as a controller necessary.[100] However, also these services can be done at processor lever, if Mydex only role is sending the data the user has requested sent, to the place where it was requested sent. Its role would not include any determining of the means or the purposes, as this is done by the user. Mydex’ role would be the technical task for sending this data to the requested party. This underlines the fluidity of the processor/controller role for PIMS.

If PIMS have a controller part in any of the data processing, this should be made very clear to the data subject, as the level of trust needed in a PIMS also means PIMS need to be extra transparent in order to be compliant with the GDPR, and in particular Article 5(1).

2.2.2 Processor

According to the Directive Art. 2(e) a "processor" shall mean "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;". In the GDPR this is unchanged in Art. 4(8). The GDPR legal obligations are imposed on processors as well as controllers both in and outside of the EU/EEA for establishments in the European Union, see Art. 3(1) GDPR and Recital 22. While the definition of "processor"

[98] Mydex (2017)

[99] Mydex CIC. (2010)

[100] Case C-131/12 *Google Spain v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* paragraphs 32-41

has not changed with the GDPR from the Directive, the compliance requirements has expanded extensively. Both for the processor and for the controller as it must make sure they only appoint processors that are compliant with the law.[101] There is also a requirement for a contract or otherwise legal binding document, with information in regards to the kind of data for processing as well as the duration of the processing to mention a few.[102]

As with the controller, any natural or legal person could be a processor. However, as to the discussion in regards to natural persons within a company acting on their own accord as a controller, this would not be an issue with the processors as any processor by definition acts on the behalf of the controller; therefore, a processor using the data for its own purposes in turn becomes a controller.

In order to be considered a processor an entity must process "personal data" and it must process this data on "behalf of the controller". To be considered a processor the entity needs to be outside the controller. The processor must do this on the controllers' behalf, meaning it must follow the instructions from the controller. [103]

For a PIMS, an outside processor could be useful when considering the multi-facet entity, a PIMS would be, and the amount of data possibly going through the PIMS. Such as the PIMS Cheap Energy Club[104] using the PIMS Allfiled as its platform for storing and accessing personal data.[105] It is also worth considering PIMS as a pure processing tool. The data subjects being the controllers of their own personal data, as mentioned with the Respect Network and Mydex as an example in chapter 2.2.1. However, this would take away from some of the core usefulness of PIMS, as a part of their business strategy often is helping the data subjects make decisions. Such as Mydex.[106]

In processing there is the possibility for a processor to have controller status for some of the data, depending on the specific instructions, meaning they go over into a joint controller status instead.[107] Some discretion is allowed the processor as well, and their level of discretion is a part of the evaluation of whether it crosses over into controller territory. Therein what level of instruction is given from the controller, what level of autonomy does the processor have apart

[101] GDPR Art. 28(1) -(3)

[102] GDPR Recital (81)

[103] Article 29 Working Party. WP 169 p. 25.

[104] Cheap Energy Club (2017)

[105] Information from 2014, it is not known if this is still the case. Allfiled (2014)

[106] Mydex CIC (2010) p. 9

[107] GDPR Art. 26

from the controller in relation to the data and how does it appear to the data subject, amongst others. [108] Processors should however take great care not to go outside of the controllers instructions, as this opens them up to the full extent of the Regulations compliance and liability obligations[109].

A cloud computing supplier, without any controlling aspect, simply making sure the system stays online and all its components functions would be a typical processor[110]. Cloud based storage is one of the suggested forms of storage for a PIMS, which is natural considering the need for storage space and security of data such a program would need.[111] Whether it is a processor or controller will depend on what else is done by the PIMS with the personal data. The probability of the PIMS acting as a pure storage unit seems unlikely considering the other compliance issues in light of the GDPR, and the need for the PIMS to have a rather active role in order to be able to advise the data subject accordingly, as would be needed by the controller. However, there are as mentioned uses of PIMS that would limit the PIMS to a processor. This would only include the personal data storage, beyond this PIMS would very easily go over into the role of controller. PIMS will for many of its uses be regarded as a controller, for the tasks such as mere storage they could be limited to processor.

2.3 Codes of conduct and certification

Codes of conduct are designed to help compliance with obligations in the GDPR regarding technical and organisational measures for data security.[112] The rules regarding codes of conduct and certification can be found in Article 40-43 in the GDPR. The EDPS in its opinion stated that the new rules regarding codes of conduct and certification are instruments that could give products like PIMS a way to make the implementation of GDPR compliance easier, by being able to offer a practical solution.[113]

Codes of conduct (CoCs) and certification works both together and apart, but they are difference in use and essence.

[108] Article 29 Working Party. WP 169 p. 33.

[109] GDPR Article 28(10)

[110] Voigt, von dem Bussche (2017), p. 20

[111] EDPS Opinion 9/2016 p. 6.

[112] Voigt, von dem Bussche (2017), p. 71

[113] EDPS Opinion 9/2016 p. 13 paragraph 56

2.3.1 Codes of conduct

Codes of conduct and the monitoring of these codes is regulated in the GDPR Articles 40 and 41. They are designed to "contribute to the proper application" of the GDPR. They are supposed to make the abstract of the GDPR more accessible and useable in the day to day business, and give a practical interpretation. [114] Article 40(2) sets out a list of particularly CoC friendly provisions in the GDPR. Amongst those is pseudonymisation, transparency, the exercise of the data subjects' rights (like objections to decisions made by automated decision making), communication of data breaches and data transfers. [115] [116] PIMS can particularly benefit from CoCs as they can be sector specific[117], meaning, PIMS as a sector could get a common CoC. They could also prepare this CoC themselves under Article 40(2), as "other bodies representing categories of controller or processors". Certain types of data could have their own CoC, meaning PIMS could adhere to already existing or adopt certain CoCs.

These CoCs are in need of constant monitoring, to ensure the PIMS is in adherence to the GDPR.[118] The CoCs is under monitoring, by mainly the supervisory authority.[119] They can suspend or exclude the infringing party from the CoC.

While CoCs adherence it not eligible as proof of GDPR compliance, if they adhere to the rules under the CoC they can easily prove they are compliant with the GDPR, at the same time as actually being compliant since the CoCs need to be approved by either the member state or by the European Commission.[120] It also gives several advantages as it by design fulfils the burden of proof in several obligations in the GDPR. [121]If a PIMS were to be part of a general "PIMS CoC", or adhering to any sector wide CoC for certain kinds of data, on behalf of the controller, the burden of proof would be satisfied. PIMS could be part of several CoCs delivering on any need the controller might have which would be covered under a CoC.

[114] Voigt, von dem Bussche (2017), p. 73

[115] GDPR Article 40(2).

[116] Voigt, von dem Bussche (2017), p. 73

[117] GDPR Article 40(1)

[118] GDPR Article 40(4).

[119] GDPR Article 41(1)

[120] GDPR Article 40(5), (9) and (10)

[121] Voigt, von dem Bussche (2017), p. 76

2.3.2 Certifications

In addition to CoCs, the GDPR facilitates the use of certifications. The certification scheme would work best, if it were to be a European Union wide certificate able to ensure of compliance with data protection across member states. The certifications are made for “the purpose of demonstrating compliance” with the GDPR, by the processors and controllers.[122] The responsibilities of the controller and processor pursuant to the GDPR does not diminish, but as with the CoC it alleviates the burden of proof.[123]

A certified controller or processor have the advantage of certified as being in compliance with the GDPR, which can have high economic value from a competitive perspective.[124] PIMS should pursue such certifications, to demonstrate to both controllers and the data subjects that their workings are in compliance with the GDPR. The use of a certified PIMS,could also help the controller to be compliant and gain certification.

It is unlikely that PIMS could service as a CoC approval body, or a certification body as they would lack the necessary impartialness, considering the processing and controller aspects of a PIMS. All in all, PIMS should use and take advantage of the benefits garnered from CoCs and certification, making it a goal to either form CoC or join as many as possible, to be as attractive as possible for the data subjects and controllers.

[122] GDPR Article 42(1).

[123] Voigt, von dem Bussche (2017), p. 77

[124] Voigt, von dem Bussche (2017), p. 78

3 Principles of data processing

Article 5 in the GDPR contains the principles for processing of personal data within the EU. Any controller falling within the scope of the GDPR need to adhere to and build their processing around these principles.[125] In this chapter we will consider whether PIMS can in any way facilitate adherence to these principles. We will evaluate any limitations PIMS have in regards to lawfulness, fairness and transparency, purpose limitation, accuracy, storage limitation, integrity and confidentiality, accountability and data minimisation. To do this the different provisions in the Regulation will be examined to see what it entails to be compliant, and do an evaluation of whether PIMS is a solution for compliance facilitation.

3.1 Lawfulness, fairness and transparency

The GDPR Article 5(1) states that personal data shall be processed "lawfully, fairly and in a transparent manner in relation to the data subject". Lawful entails that the data can only be processed when it is done on legal grounds or by the users' consent.[126] Fairness requires the controller to be fair in their relation to the data subject, meaning being transparent with their intent for use, handle the data as can be reasonably expected and not misuse the data.[127] Within transparency lies the requirement that the data subject is able to easily access and understand the processing.[128] Including the identity of the controller, and the purpose and reason for their personal data being processed, as well as any other information that could be relevant for the data subject to ensure their data is protected.[129] The controllers are also required to make the data subject aware of "risks, rules, safeguards and rights" relating to the processing of their data, as well as how they can exercise their rights.[130]

These principles, together with the rest of Article 5, read as the backbone of the GDPR as far as how the rest of the regulation should be read and interpreted.

The use of PIMS for a controller would help the controller be compliant with the principle of transparency in the Regulation. PIMS is in its essence, a transparency conduit, which controllers should be willing to use to ensure and demonstrate they in fact are doing what they can to adhere to the principle of transparency. Some PIMS also market themselves to potential users

[125] Voigt, von dem Bussche (2017), p. 87

[126] Voigt, von dem Bussche (2017), p. 88

[127] UK Information Commissioner's Office on Processing fairly and lawfully. (2017)

[128] GDPR Recital 39

[129] GDPR Recital 39

[130] GDPR Recital 39

as a transparent system, such as the PIMS Midata which on its front page has transparency listed as a benefit of using their PIMS.[131] This they achieve through having their governance principles public, and allowing the members to take part in the decision-making process.[132] [133]

Further, PIMS give the data subject an overview of their data, as well as all information needed, in a setting where the data subject expects it. The setting provides legitimacy as there is no doubt as to what considerations the data subject is doing, where a basic functionality is to manage ones' data. This is relevant for the evaluation of consent since the consent need to be a "freely given, specific, informed and unambiguous indication" of the data subjects wishes. The fact that the decision is made through a PIMS, can strengthens the controller's argument that consent was correctly gathered.

3.2 Purpose limitation

According to Article 5(1)(b), personal data should be collected for "specified, explicit and legitimate purposes", and " not further processed" unless this processing is compatible with the original purpose of the collection of the data. There are exceptions for further processing in relation to "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", Article 5 here references Article 89(1).[134] The purpose for the data processing is a key provision for evaluating whether the data is processed in accordance with the other principles of data minimisation, accuracy and storage limitation.[135] The Regulation text is unchanged from the DPD Article 6(1)(b), except from some additional safeguards in GDPR Article 89(1)and the codifications of the compatibility evaluation, so the Article 29 Working Party's opinion on the provision will be central to the discussion.[136]

Purpose limitation is twofold, in that it serves the data subject in how it is designed to limit the use of their data beyond their original purpose, as well as it serves the controllers in that it opens up for further use within certain parameters.[137] The question for this thesis is whether there is any room within that space, where PIMS could simplify or better the use of this space for either controller or data subject. This would be a field where if PIMS proves useful, it could be easier to gain traction with larger businesses as the further use of data at the same

[131] Midata

[132] Midata

[133] Midata (2017) p. 2

[134] Forgó, Hänold and Schütze, (2017), p. 34

[135] Voigt, von dem Bussche (2017), p. 88/89

[136] Article 29 Working Party. WP 203

[137] Article 29 Working Party. WP 203 p. 3

grounds as before as well as would lessen their costs. Specific discussion of further processing in chapter 3.8. First we'll discuss the purpose itself, and go on to the limitations of that purpose.

3.2.1 Specification

Firstly, the purpose for the initial collection of data needs to be specified. Purpose specification is central to the purpose limitation as it sets the boundaries the controller has to adhere to when considering further processing. They also have to be able to document their compliance with specificity by showing they have made an internal assessment of the need for this data, therein what it is to be used for, taking care to not get irrelevant, inadequate or unnecessary data.[138]

PIMS could be useful here, specifically considering the data which relate to "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", which could be predetermined. In particular if the member states' Data Protection Authorities (DPAs) has taken an active role in the PIMS, as they could have first-hand authority on what kind of information would qualify as these in the given member state.

The degree of specification depends on the context.[139] In any case, it needs a certain degree of detail for the data subject to be able to pinpoint what kind of processing it is, and if it isn't within the purpose. [140] Vague or general purposes is therefore usually not accepted, and not seen as being "specific". The evaluation is therefore always a balance between too much detail, which is also not advised[141], and enough detail. The WP29 in their opinion WP203 on purpose limitation recommends a "layered notice", giving the data subject the choice of how much they wish read.

PIMS could be useful in informing the data subject on behalf of the controller. I.e. if a new company selling computers, where the company has data that was gathered for transactions, and wishes to further process that data for their own analysis, it could be easier to use a PIMS to relay this information as a request specifying at time of purchase that the data may be used for analysis. Some PIMS also offer businesses access to this data in anonymised form[142]. This is especially relevant if the company is new and without much resources or knowhow on how to do this and still be compliant. PIMS could be a good partner for any new start-up, assisting

[138] Article 29 Working Party. WP 203 p. 15

[139] Forgó, Hänold and Schütze, (2017), p. 27

[140] Article 29 Working Party. WP 203 p. 15

[141] Article 29 Working Party. WP 203 p. 16

[142] Trust Hub. (2016)

in counselling on how they should design their data usage and gathering and still remain compliant. Such as the PIMS Bits About Me, who offers the businesses markets compliance with the GDPR, which will inter alia include the limitation of the data based on gathering only for the specific purpose needed.[143]

An issue is that the controller would have to do the purpose specification evaluation in each instance, which for some controllers would mean it would most likely makes as much sense to do it themselves. For instance, in companies with large intricate one-time transactions. However, if it were frequency transactions, and what data would need a certain kind of specification was predefined, PIMS could use this for each identical or near to identical processing. The controllers will have done an evaluation for their data and have an easy way to document it with help of a PIMS, and be compliant with the transparency principle and the purpose limitation specificity principle, as well as being able to document in regards to the burden of proof. The controller itself should be responsible for providing documentation on the specification of the data collection.

3.2.2 Explicit

Secondly; the purpose must be explicit. This means the purposes in addition to be specified, must be explicitly clear towards what the actual purpose is. This should happen at the time of the collection of data.[144] The WP29 underlines the importance of the language not being vague and easily understandable by all possible parts of the data collection and its following use.[145] It is meant to build under the transparency principle, and predictability.

The means of informing the data subject of the specific and explicit information regarding the collection of data, is a PIMS suited task. While the specificity and the explicitness of the purpose would need to be decided by the controller, PIMS could do the actual informing towards the data subject. The legislation opens up to several ways to do the actual informing.[146] The OECD Explanatory Memorandum to the Guidelines[147] mention as examples " public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies.". PIMS could easily have any of these roles, this is the exact kind of information that should be given through the PIMS. And as it is in a setting where the user is expecting data protection queries, the user will be highly aware that this is in relation to its data security, which is beneficiary to any controller facing having to document their purpose

[143] Bits About Me (2017)

[144] Article 29 Working Party. WP 250 p. 17

[145] Article 29 Working Party. WP 250 p. 17

[146] Article 29 Working Party. WP 250 p. 18

[147] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, paragraph 54

was specified and explicit in a way the data subject was sure to understand, and the burden of proof.

3.2.3 Legitimate

Third; the purpose must be legitimate, meaning it must be compliant with all law and regulation. As stated in recital 40 of the GDPR in order for processing to be lawful, the processing must be done based on consent, law or "some other legitimate basis". This is meant to be interpreted broadly, at least in relation to purpose legitimacy.[148] This would require an evaluation of whether the data processing and collection of data is compliant with the law or part of an agreement with the controller. Several PIMS market themselves to businesses as an advisor to legal compliance, for example Bits About Me, which markets themselves to potential business clients as delivering "GDPR as a service" and that outsourcing GDPR compliance can be a way to avoid high fines. [149]

3.2.4 Compatibility

The use of the data must not be "processed in a manner that is incompatible" with the purposes just described, Article 5(1)(b). This allows for slight changes in the controllers use of the data, for the same purposes as collected.[150] The GDPR also opens up for processing of data for a new purpose in Article 6(4), which will be discussed in chapter 3.2.5. The compatibility consideration the controller must do here is not a checklist consideration, followingly, PIMS as a processor would not be suited to preform that evaluation, but could be useful for informing the data subject of any slight change in use under the same purpose when considered as compatible with the controller.

There is also opportunity for the controller to do further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[151] All these needs further decision as to whether the processing in question falls within one of the exceptions to the general purpose rule. The point with the exceptions is that broadly speaking the controller should be able to do this without informing the data subject. Further, the provisions can be interpreted quite broadly when reviewing recital 158-162.[152] However, if through a code of conduct the PIMS could also do these.

[148] Article 29 Working Party. WP 250 p. 20

[149] Bits About Me (2017)

[150] Article 29 Working Party. WP 250 p. 21 and GDPR recital 50

[151] GDPR Article 5(1)

[152] Forgó, Hänold and Schütze, (2017), p. 36

3.2.5 Further Processing, different purpose

In their process the PIMS would have to uphold its requirements for "further processing", and requirements in regards to purpose limitation. Whether further processing for a purpose other than what the data initially was collected for is compatible with the original purpose has to be considered with the provisions in GDPR Article 6(4).

The provision that need to be considered is first whether there is any link between the purpose for the initial collection and the further processing. This may be the case where the data was initially collected for information purposes under a census or similar, and would go through further processing for anonymisation for further use.[153] Secondly, one can take into account the context of the data collection, and the relationship between the data subject and the controller.[154] Third, the nature of the personal data needs to be considered, this includes special consideration for data pursuant to Article 9 and 10. As previously discussed explicit consent as required by Article 9 would be natural to go through PIMS, so should the controller wish to do further processing the consent would already be in place for the original processing. The consideration would then be whether the consent is compatible with the further processing. It would be simplest if the PIMS could get pre-approved the most usual cases in order to make the process as smooth as possible.

The fourth consideration point; Article 6(4)(d) would perhaps be problematic for PIMS as it entails a risk calculation. The article sets to take into account the “possible consequences of the intended further processing”. One option would be to present the data subject with possible known risks for this type of further processing; however it is unlikely that the businesses and organizations would be neutral to what information would be shared here. This can be a part of the trust based system PIMS promise their users, as the Respect Network promises its users.[155] A possible solution could be getting the information from a third party, like the member states DPAs. This would however need cooperation and collaboration between government, PIMS and the organization/businesses partaking, echoing the sentiment from the EDPS Opinion in PIMS.[156]

Finally, in Article 6(4)(e), the “existence of appropriate safeguards, which may include encryption or pseudonymisation” is promoted. According to Recital 50, this includes both the original and the intended further processing. So, if there are high levels of encryption or the data is pseudonymised, this will likely count in favour of further processing. Several PIMS

[153] GDPR Article 6(4)(a).

[154] GDPR Article 6(4)(b).

[155] Respect Network (2017)

[156] EDPS Opinion 9/2016

market themselves as high on security, therein encryption, which could help facilitate further processing for the controller.

The issue with further processing and PIMS, is that Article 6(4) opens up for further processing on the same legal ground. In which case the PIMS would mainly function as an advisor to businesses and organisations, and would not need for the data subject agree or even know about the further processing. Considering how the PIMS is mainly supposed to be a way for the data subject to control how their data is used, even if the controller can continue processing on the same legal ground, data protection forward controllers could use PIMS as an information channel to their data subjects informing them that their data will be further used in compliance with regulation. This also supports the GDPRs general goal of better recourse opportunity and protection of their rights and data to data subjects.

3.3 Accuracy

The GDPR Article 5(1)(d) constitutes that data shall be "accurate", as well as "kept up to date". The controllers are expected to take "every reasonable step" in order to make sure the data processed reflect the facts. When considering whether the steps in question are reasonable, the purpose of the data is a point of evaluation. If the data is found to be inaccurate the data is to be "erased or rectified" without further delay. The principle is found also in the GDPR provisions regarding rectification and erasure.

This is an underlying principle of GDPR that PIMS is suited to support. Keeping the data up to date and accurate, is a key value for almost all PIMS as a selling point for good quality data. Such as Mydex, who states: “The central flaw is that organisation-centric approaches can never ensure that the data in question is accurate, complete or up-to-date.”[157] The data subject going into their personal information management system to update their data, while at the same time knowing what and why they are updating benefits the controller largely. And the data is undeniably most accurate when coming directly from the data subject. It would also be easy for the controller to send out an alert through the PIMS to verify the data they have is correct, and the ever-updated personal data is also sold as a pro from the PIMS.[158] In order to make sure the limits of purpose limitation are followed as well, the PIMS could have settings for certain controllers limiting what level of data access they are to have. All depending on the type of data, data subject preferences and other relevant regulation and special pro-

[157] Mydex CIC. (2010) p. 21

[158] Mydex CIC. (2010) p. 26

visions, either decided by the data subject or automatically by PIMS.[159] All in all, PIMS would support this principle as well.

3.4 Storage limitation

Article 5(1)(e) sets boundaries to how long the controller is allowed to keep data in a form "which permits identification". The controller cannot keep the data "for longer than is necessary for the purpose for which the data are processed". There are exceptions to the rule for processing "solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".[160] GDPR recital 39 states that time limits should be established by the controller, in order to review and either erase or make sure the data is still needed and within the boundary of necessity for the purpose. However, the data subjects right to erasure can mandate erasure of the data before the time following from the purpose.[161] [162]

There are several technical or time determined aspects which a PIMS could facilitate. For example: the data is collected in order for the controller to fulfil a contract, when the contract is fulfilled a PIMS could inform the data subject the contract was fulfilled and whether the controller was still retaining the data subject's data. In which case the data subject could easily send a notice requesting erasure or consent to further processing. Or the controller can have a retention policy in place which could be entered into the PIMS and executed automatically.[163] However, this would need for the contract to be fairly simple, and for other more complicated grounds a PIMS is not likely to have the necessary insight in order to inform the data subject whether the purpose for the retention of the data was "exhausted", where the PIMS is not the controller itself. A PIMS would still be able to keep the data subject in the loop in a user-friendly manner, simplifying the process both the controller and the data subject would need to go through by acting as an intermediary with a user-friendly interface. This also supports the transparency principle. A PIMS as a processor would in any case, not be able to decide what is "necessary" as the law opens up for in regards to the controller.

[159] Such as a model openPDS/SafeAnswers markets itself to users with

[160] See GDPR Article 89(1)

[161] Voigt, von dem Bussche (2017), p. 92

[162] GDPR Article 17

[163] Voigt, von dem Bussche (2017), p. 92

3.5 Integrity and confidentiality

The personal data according to Article 5(1)(f) shall be processed so that it ensures "appropriate security" for the personal data. This includes "protection against unauthorised or unlawful processing" as well as against "accidental loss, destruction or damage". The breach of this principle can be potentially very damaging, as a consequence could be data breach as it relates to protection of the data from unwanted parties.[164] The substantiation of this principle in the GDPR is the organisational requirements as this principle is related to compliance and data security. Most PIMS use this in their communication to individuals in their marketing as a key part of their product. The Respect Network states that “No one can use those assets without your express permission so the ability to buy, sell, or trade your data is limited by design.”[165] As well as Bitsabout Me that is clear towards its users that “We keep your data safe, secure and private”[166]. These PIMS implement technical solutions to make sure only the users can access and use their data unless they choose otherwise. They also underline the fact that they keep the data secure, such as Trust Hub which lists security as a key value on their home page.[167] This will in turn also benefit businesses as they are obligated under the GDPR to uphold these principles, showing they use a PIMS to ensure the data of their users is safely stored and secured.

3.6 Accountability

Accountability is in essence, the responsibility the controllers have for the data subjects' data, and the codification of the responsibility for compliance with the Regulation tied in with consequences for breaching this principle, for the controllers. Accountability is codified in the GDPR under Article 5(2). The controller must also be able to prove their compliance to relevant supervisory authorities.[168] The accountability of the controllers was the main focus of the WP29 Opinion WP173, suggesting that accountability measures could be a way to move data protection from abstract to practise in a way that effectively protect the data.[169] The GDPR has several of the WP29 suggestions implemented to enhance accountability, amongst those the principle in itself, impact assessments and data protection officers. Data protection by design and by default is also an important part of accountability[170]. As Article 5(2) makes

[164] IT Governance Privacy Team (2017), p. 114

[165] Resptect Network (2017)

[166] Bitsabout Me (2017)

[167] Trust Hub (2017)

[168] Voigt, von dem Bussche (2017), p. 31

[169] Article 29 Working Party WP 173 p. 3 paragraph 1.

[170] Article 29 Working Party WP 173 p. 11 paragraph 41.

controllers accountable for upholding the principles for processing under Article 5(1), the controllers need to be able to document compliance with all of them and the material and organisational obligations in the GDPR.[171]

One of the main components with the accountability principle, is the controllers need to be able to document compliance. PIMS is a very effective tool for documenting compliance, which is a selling point for PIMS. For example, Trust Hub offers an “Comperhensive audit-trail”.[172] PIMS will in order to demonstrate they provide compliance with regulation be able to, for example, provide the businesses with documentation of the right to access[173], as access to personal data at any time is a basis of PIMS as a product. Also, when used in informing of a data breach, PIMS could provide the businesses with the logs showing each user received appropriate information regarding the breach.[174] PIMS could in some cases be more than is necessary as it builds on close communication with the data subject and a user-centric model. This should not be a reason to not use PIMS. The general use of systems such as PIMS would count in the controllers’ favour, as intent would be part of the evaluation of the controllers' responsibility, and the measures taken to be compliant.[175]

3.7 Data minimisation

Data minimisation is a main principle in the GDPR, as follows by Article 5(1)(c). The personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ".[176] The data controllers therefore need to review that the data they are collecting is adequate in regards to the purpose they are intended for, and evaluate whether the data collected is proportionate when seen together with the intended processing.[177] As data minimisation is an important right for the data subjects, which is highlighted when PIMS market themselves to the users. Such as openPDS/SafeAnswers informs on their website: “Only the answers, summarized data, necessary to the app leaves the boundaries of the user’s PDS”. [178] As for controllers; using PIMS to help the data subject keep control over their data is certainly in spirit of the principle, and would count positively towards

[171] Voigt, von dem Bussche (2017), p. 32

[172] Trust Hub. (2016)

[173] GDPR Article 15

[174] GDPR Article 33 and 34

[175] GDPR recital 39

[176] See also GPR recital 39

[177] Voigt, von dem Bussche (2017), p. 90

[178] openPDS/SafeAnswers (2017)

adherence to the data minimisation principle as this allows the data subject to themselves control how much and for how long and in what manner their data is utilized.

4 Key provisions

4.1 Consent

4.1.1 Affirmative consent Article 7

Where the data processing relies on consent from the data subject as is stated in GDPR Art. 7(1), there are new more stringent rules for compliance than what was in the Directive. Where the Directive was more lenient in regards to consent[179], the GDPR has more concrete provisions, with the advantage of being identical in all member states.

Now the consent must be given by "clear affirmative action", see GDPR Art. 4(11). It must also be "informed and unambiguous". The request for consent must be "clear" and "concise".[180] If consent is given as part of a contract, i.e., which also concerns other matters the request for the processing should be "clearly distinguishable" from the rest of the contract.[181] This would be applicable for the processing not concerning the performance of a contract. In an assessment of whether consent is freely given the GDPR gives weight to whether consent was requested in a contract where the requested data was not necessary for the performance of that contract.[182] The data subjects should as easily as they gave their consent be able to withdraw they consent,[183] the controller also need to inform the data subject that they have the right to withdraw.

PIMS could here definitely be of very good use to the data subjects, as well as the services who today can only be said to take advantage of the freer current rules for data processing. As Mydex points out, it is easy to overlook the “small print” in an agreement. And want to reverse this process, making the data subject able to specify the information they wish to share and with who they wish to share it with. [184] This would fulfil the requirements in the GDPR, as well as placing the data subject in control.

Another positive for the data controller or processor, in the use of PIMS to gain consent, is the burden of proof under GDPR Art. 7(1). The burden of proof that proper consent has been received, lies with the controller. If a data subject claims it has not given its consent, it is the controller who must prove it has. This is a direct market strategy for PIMS providers, offering

[179] Article 29 Working Party. WP 249 p. 11 and 21

[180] GDPR recital 32

[181] GDPR Art.7(2)

[182] GDPR Art. 7(4)

[183] GDPR Art. 7(3)

[184] Mydex CIC. (2010) p. 10

their users to control their consent through the PIMS, which also provides the businesses with proof of consent and compliance with the Regulation. Such as Mydex offering their users the ability to “review the default settings for which pieces (fields) of data are shared (e.g. name and address, but not telephone number) and whether this is automatic or requires your permission each time.”[185] This information could then be used to document the data subject has given affirmative consent. This is also an instance where it would be beneficiary for the PIMS to be part of Codes of Conduct or to be Certified.

4.1.2 Explicit consent Article 9

Explicit consent was also required under the DPD to process certain kinds of data. In the GDPR Art. 9 is the need for "explicit" consent for processing of "special categories of personal data", Art. 9(a). PIMS could be useful in these situations, as they are supposed to have more accurate data due to the data being entered and monitored by the data subject itself. Therefore, answers to these questions could facilitate the need for explicit consent. There are also several other exemptions from the general prohibition of the processing of these data. [186] PIMS could keep track of these in combination with the information above and process data accordingly or advice the controller. In the new GDPR personal data has been expanded to include genetic data and biometric data[187].Genetic data and biometric data are defined in Article 4(13) and (14).

A PIMS would have the necessary knowledge, or should strive to make this a part of their business model, to identify what data can be construed as genetic data and biometric data, which is not something data subjects would know without further information, as the methods they use for biometrics are highly sophisticated and requires much less information to identify than one would think. This could be done by questioners tailored to get this information, with the knowledge of the data subject. If successful they would be able to help the data subject protect this data and make sure they took extra caution before sharing this. As well as advising new businesses that these types of data have extra consent requirements.

4.2 Anonymisation and pseudonymisation

When it comes to anonymisation and pseudonymisation PIMS seems to be in a particularly good situation, enabling the controllers to have access to data without any of the, or just some of, the provisions under the GDPR be applicable to them.

[185] Mydex (2017)

[186] Maldoff, (2016)

[187] GDPR Article 9(2)

4.2.1 Anonymisation

Anonymisation is the absolute irreversible removal of possibility of identification in the data. According to the GDPR recital 26, in order for data to be anonymous the data cannot relate to an identified or identifiable natural person, and needs to be "rendered anonymous in such a manner that the data subject is not or no longer identifiable." If the data is truly anonymous, the GDPRs rules does not apply, as the GDPR applies to personal data only. According to the WP29[188] however, a sufficient degree of anonymisation is very hard to achieve. In addition to the risk of re-identification in later processes and of third parties identifying the data subject with new data.[189]

The anynomisation of the data is in itself considered processing. Assuming the data was gathered for a purpose, the anonymisation is a case of further processing. All processing and controlling up until the point of data anonymisation falls under the scope of the GDPR and needs to follow the regulation accordingly, meaning it needs to fulfil one of the requirements for "further processing" in Article 5 or 6. However, the WP29 reasons that any anonymisation as further processing can be considered "compatible with the original purposes of the processing", but only as far as the anonymisation process reliably produces anonymous information, as described in their opinion on anonymisation.[190] Meaning; anonymisation could be done with coverage under the GDPR Article 5(1)(b), which again means that this could be outsourced to PIMS. This opens op the anonymisation possibilities much more than if anonymisation was seen as incompatible with the original purpose as a main rule.

Trust Hub offers anonymisation as a service to their users, as part of their PIMS package.[191] The data would also have to be stored for a while as is required for the data subject to retain the right of access to previous processing.[192] If a controller has outsourced their anonymisation to a PIMS, where the data subject would have the opportunity to keep tabs on their data, the PIMS will be able to take the obligation of storing this data without the controller being in risk of not being compliant with the GDPR.

As mentioned, it is very hard to anonymise data to the degree that data subjects cannot be identified, at the same time as the data remains useful. This needs to be balanced out with the actual standards set by the GDPR: the data can no longer identify a natural person, by "all"

[188] Article 29 Working Party.WP 216

[189] Article 29 Working Party WP216 p. 12

[190] Article 29 Working Party WP216 p. 7

[191] Trust Hub. (2016)

[192] Case C-533/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* paragraph 64

means that are "likely reasonably to be used" and the processing must be irreversible.[193] The greatest risk for a PIMS, who is hired by data subject and controller to anonymise personal data, is leaving too much residual information so that re-identification is possible. Such as the application CitizenMe which sells surveys the users can earn money from, which gives the users the possibility to do this anonymously,[194] is dependent on their users actually remaining anonymous. Otherwise they would have broken the law as well as suffer a severe breach of trust and their whole business is no longer viable. This means any technique the PIMS use, must be generally seen as sufficiently secure for them to ophold their responsibility in anonymising the data.

4.2.2 Pseudonymisation

Pseudonymisation is not as definite as anonymisation. Pseudonymisation is when the data can no longer identify the data subject without addition information.[195] The identifiable data needs to be kept separate from the pseudonymised data, and there need to be technical and organisational separation measures to ensure the data is not attributed to an identifiable person. Unlike anonymised data pseudonymised data falls within the scope of the GDPR.[196] However, pseudonymisation is one way for the controllers, perhaps through PIMS, to adhere to their responsibilities in the GDPR while still keeping the data more useful and more valuable than with anonymisation.

While the GDPR still applies to pseudonymised data, it has several incentives for those choosing to pseudonymise their data. GDPR recital 29 emphasizes the incentives by stating that "to create incentives" to pseudonymisation "measures of pseudonymisation should, whilst allowing general analysis, be possible".

One incentive is found in Article 6(4)(e); which factors in the allowance for further use of the data where data is further processed in a "compatible" way when seen with the original purpose of the gathering of the data. Meaning, controllers who pseudonymized their data on entry as a rule, would be more likely to benefit from the provision in Article 6(4)(e). This is also a part of the GDPRs data protection by design, or code[197], and could be a safeguard as mentioned in Article 25. PIMS could keep identifiable information, this requires no legal evalua-

[193] Article 29 Working Party. WP 216

[194] CitizenMe. (2017)

[195] GDPR Article 4(5)

[196] GDPR recital 26 and 28

[197] Lessig (2006)

tion and would be a pure technical service, as well as it would most likely improve the weight the controller could put into the factor in Article 6(4)(e). [198]

Further, Article 32 implements the need for controllers to establish risk-based measures for protecting data security: pseudonymisation is one such measure.[199] Should there be a security issue that is regarded as "a risk to the rights and freedoms of natural persons"[200], or if the risk is "high",[201] the controllers need to inform the data subjects. However, if the data is pseudonymized the need to inform the data subject may be avoided. This also applies to the possibility for the controller to be free of the provisions in Article 15 through 20, see Article 11. [202]
PIMS offer pseudonymisation services to their users. This is particularly attractive to businesses as this provides leniency for the GDPR. Such as the PIMS Trust Hub which offers "data masking", which includes pseudonymisation. [203] This would probably be part of a servicing package, and one would need to adhere to the Regulation in full up until the data is properly pseudonymised. PIMS offering their pseudonymisation services as a part of a total servicing package therefore makes sense.

Should PIMS be utilized here, they could easily inform all data subjects, even with pseudonymisation in place. PIMS can be used by the controllers to fairly easily not have to inform of any such risk if they have pseudonymisation in place. However, it is more in "the spirit" of the GDPR to inform of such risk anyway for PIMS users as it is natural information to receive in such a program, and as mentioned most of them are trust based. [204]

4.3 Breach notification

The GDPR Article 33 and 34 gives the data subjects a new right to receive information when there has been a breach to their personal data. The Regulation defines personal data breach as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[205] This also includes accidental breaches.[206] In the case of a personal data breach the

[198] Maldoff (2016)
[199] GDPR Article 32(1)(a).
[200] GDPR Article 33(1)
[201] GDPR Article 34(1),
[202] Maldoff (2016)
[203] Trust Hub. (2016)
[204] i.e. Mydex puts weight on trust in their product: Mydex CIC. (2010) p. 26
[205] GDPR Article 4(12).
[206] Voigt, von dem Bussche (2017), p. 65

breach is to be reported to the supervisor authority[207] without “undue delay” and "no later than" 72 hours after having become aware of the breach, unless the breach is "unlikely" to be a risk to the rights and freedoms of natural persons.[208] Within 72 hours might therefore be too late as it may still be an “undue delay”, depending on the data[209]. The processor is not obligated to report to the supervisor authorities, but to the controller.[210] If the data breach is considered “likely to result in a high risk” to the rights and freedoms of natural persons, the controller is obligated to inform the data subject directly, without undue delay.[211]

While PIMS can do little in regards to identifying a data breach - unless it is the PIMS itself suffering from a breach, in which case the rules would also apply to the PIMS – the actual notification of the data subject has several regulated requirements listed in Article 33(3), ref. Article 34(2). It should (a) describe the nature of the breach, (b) inform of a contact point for the DPA or other contact point, (c) describe likely consequences of the breach and (d) describe what measures have been taken or is proposed to be taken to address the breach with possible measures to mitigate adverse effects. The WP29 recommends dedicated messages when communicating the breach to the data subjects, and that the controller should choose methods that “maximizes the chance of properly communicating information to all effected individuals”. [212] The need for individualised information will increase with the type and severity of the data beach. PIMS could in the event of a data breach be able to inform their users immediately, by sending them a message in the system, informing them of a breach of their personal data. The need for the data subject to be quickly informed could be supported by, i.e. text messages from the PIMS. PIMS by the standards explained in the GDPR and the WP29s decision seem to be qualified to deliver the message in way that makes the controller compliant with the GDPR as far as the means of communication goes, and that in any degree of the severity of the data breach. As well as having the advantage of the data subject being aware of receiving information regarding their data de facto in the PIMS, the need for an easily understandable language could be a service provided by PIMS. If they were to get the necessary information from the controller, the PIMS should be able to formulate a communication that is easily understandable. This is therefore a key provision of the GDPR where PIMS could prove highly useful and support data protection.

[207] See GDPR Article 51

[208] GDPR Article 33(1).

[209] GDPR Recital 87

[210] GDPR Article 33(2)

[211] GDPR Article 34(1).

[212] Article 29 Working Party. WP 250 p. 18

4.4 Right to access

The data subject has according to GDPR Article 15 the right to access their personal data from the controller. They have the right to "obtain" information from the controller on whether personal data concerning the data subject are being processed, Article 15(1). If the controller is processing the data subjects' personal data they have the right to access to this data and information as is mandated in Article 15(1)(a)-(h), including the purpose, categories of data, recipients of data, duration of data storage, knowledge of the right to erasure, the right to lodge a complaint, the source of the data and the existence of automated decision making. The provision grants extensive rights to the data subject.

Instead of the request going directly to the controller, a more efficient solution would be for the controller to utilise PIMS. If the controller were to handle each of these requests individually, this could potentially be very cumbersome and resource demanding. However, if the controller were to request their users to send their data to the controller via PIMS, or use PIMS as a data provider or processor, all the data could be catalogued on entry, and many of the rights pertaining the right to access would solve themselves. Available for the data subject on their login and request of information. As the PIMS system is user centric with its own user interface for the data subjects, this would work no matter what system the controller has internally. Making it a selling point worth noting for PIMS. As long as the controller supplies the PIMS with the necessary information before they start using PIMS as data collection, all information could be extracted and delivered with speed and ease. Which is a point in itself in the GDPR: data protection is supposed to be easy. If any private or governmental PIMS business want to get traction in a market where the companies with the most need for data are the ones with the largest needs in regard to GDPR, they should build upon the right to access, and bridge out from there to other provisions of the GDPR which PIMS could support. Personal information management systems should view this provision as central to their success.

4.5 Right to be forgotten (right to erasure)

The right to be forgotten was introduced by the Court of Justice in the *Google Spain*[213] decision.[214] The right to be forgotten was then codified by the GDPR in Article 17. According to the GPR the data subject shall have the right to get "erasure of personal data" and "without undue delay". In addition to the data subjects right to have its data erased, the controller has

[213] Case C-131/12 *Google Spain v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

[214] Voigt, von dem Bussche (2017), p. 156

the “obligation” to – also – “without undue delay” erase the personal data under further specified grounds. These are listed in Article 17(1)(a)-(f).

With PIMS it is the data subject itself that has ultimate control over their data. This includes the right to remove the data when they please, as with the Respect Network which gives the users full ownership and control over their personal data.[215] The right to be forgotten is therefore highly compatible with PIMS, as it gives the user this right continuously as part of its basic operations.

However, the data also has to be stored for a time so it can remain accessible for the data subject, in order for the data subject to be able to exercise their rights in the Regulation, for past processing. This was decided by the European Court of Justice in *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*[216] ruling that according to the DPD it was required to ensure right of access by storing the data for a fixed period of time, in order to keep a "fair balance" between the interests of the data subject and the burden on the controller to store that information.[217]

4.6 Data portability

Under the GDPR the data subject will have the right to data portability. According to the Regulation, the data subject can ask of the controller, for their data to be either handed back to them, or directly to another controller, where this is technically feasible.[218]

This will most likely cause quite a workload for some businesses, as the Regulation requires, amongst other things, the data to be provided in “a structured, commonly used and machine-readable format”. Meaning that where businesses don’t have a way to structure their data in a commonly used format, such as an excel file or CVS file, they need to start making these procedures in order to be compliant. Some companies use PIMS as a way to promote their consulting services, in relation to data portability and how this right makes businesses vulnerable, and underlines the need to build up trust, by the use of such systems.[219] However, any data portability right would be meaningless if the data subject had no way of understanding the data handed back to them. PIMS could here be useful as a middleman between the controller and the data subject, in that the controller could send their data to and through the PIMS for

[215] Respect Network (2017)

[216] Case C-533/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*

[217] Case C-533/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* paragraph 64

[218] GDPR Article 20

[219] Evry (2017)

“translation” to a format understandable for the data subject. In addition, PIMS would already have all the data for the user stored, and the user can move this data whenever they want. As is promoted by the Respect Network which as part of their trust network promise from member to member to “ensure the portability” of their personal data.[220]For a controller who has broadly used technical solutions, outsourcing this to a mutually - between the data subject and the controller - agreed party as a PIMS, would probably be cost saving. And if the PIMS already keeps the data for the data subject, it’s even easier.

The Article 29 Working Party has stated in their guidelines on the right to data portability[221] that the right of the data subject is a wide reaching one, and includes raw data

PIMS as a processor could have a hard time solving the direct transfer issues, as the transfer is inherently without a third party other than the other controller. The GDPR Art. 20(2) gives the data subject this right. However, this provision only applies where this is “technically feasible”. There could be a possibility, under the technical feasibility, to require the transfer to go through a service like PIMS, in order for the data to go as directly as possible between controllers, without the data subject having to do anything themselves. This would have to be with the consent of the data subject. Where transfer is not technically feasible, the data controller has the option to give the data directly back to the data subject, PIMS would for most data subjects most likely seems as a good solution as opposed to get raw data. Although the controllers are encouraged by the GDPR in recital 68 to develop interoperable formats, this is not an obligation.[222]

In the UK one PIMS initiative does data portability. This initiative is called Midata, and it relates to banking.[223] Consumers get the data businesses has on them in an understandable format. They can then upload this data to compare what services would best suit their needs, i.e. for banking and cell service.[224] The UK ICO also recognizes, as the European Data Commissioner, the need for government to step in and take an active role in setting the stage for a community where data protection law is upheld. As well as stating Midata has considerable overlap with the provisions for data portability in the Regulation. [225]

[220] Respect Network Blog (2012)

[221] Article 29 Working Party. WP 242

[222] Article 29 Working Party. WP 242 p.5

[223] UK Department for Business, Innovation & Skills (2011)

[224] UK Department for Business, Innovation & Skills (2011)

[225] UK Information Commissioner’s Office on Midata (2017)

The GDPR also protects any third parties right to data protection in Article 20(4). If the transference of the data for the requesting data subject, prevents the right of the third party to exercise their right as data subject, this would be considered an adverse effect.[226] They would then have to find other legal ground to transfer their personal data as well, within the GDPR. Any processing that is by the control of the data subject, is also the responsibility as so far in as it is not decided by the controller, but only by the requesting data subject, in the context of personal activity, personal or household needs GDPR Article 6(1)(f). Also, practice should be the exclusion of data concerning other individuals, or consent mechanisms. [227] In the case where third-party information is involved, PIMS could act as a gateway also for these issues. By asking the data subject and the controller, if they have made sure the move of this data to different processing does not concern of jeopardize the rights of another data subject pursuant to the GDPR. This type of information can easily go under the radar, as the third party won't necessarily be made aware of any goings on with another person, unless the data is so undeniably personal that a consent request is spurred without further consideration.

4.7 Automated decision-making - profiling

"Profiling" is defined in the GDPR Article 4(4) as "means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person,".

Data subjects has particular rights in regards to profiling, most central to the GDPR the rights to object, stop the profiling and not be subject to profiling based decision. The GDPR restricts automated decision-making in its Article 22. The right is not necessarily the right not to be profiled, but to control the outcome and decisions based on the profiling. Profiling and automated-decision making are to be differentiated, as profiling have a wide definition, as is apparent from the GDPR and from the WP29.[228] According to Article 22(1) the data subject has the right to "not to be subject to a decision based solely on automated processing, including profiling". The decision must have a legal or effect or similar to legal effect on the data subject, for example like stated in recital 71, " automatic refusal of an online credit application". Meaning, the profiling in itself is allowed, but to make decision based on it is not. What level of "human intervention" as stated in recital 71 is needed for the decision making not to be automated is unclear. If PIMS is allowed to do some of the information stream necessary to the data subject, what level of human interaction the decision has had is relevant for the information provided the data subject. PIMS could offer controllers benchmarks of human in-

[226] Article 29 Working Party. WP 242 p.11

[227] Article 29 Working Party. WP 242 p. 11 and 12

[228] Article 29 Working Party. WP 251 p. 5,6 and 7

tervention securely within the parameters, and in the process providing the controllers the documentation needed to prove compliance.

Article 13(2)(f) regulates what information is to be provided to the data subject at the time "when the personal data are obtained", in regards to profiling. The controller is to inform the data subject with the information of the "existence of automated decision-making", and therein the "logic involved" and the significance this has for the data subjects' data and the processing, as well as the possible consequences to the data subject of such processing. This is an ideal PIMS task, as the main purpose of PIMS is to make sure the data subject has necessary information regarding their data and particular processes in one place. The WP29 states the controller should relay simple but meaningful information to the data subjects.[229] PIMS could service both controllers and data subject by taking on the task of writing and relaying this information. The same applies to Article 14(2)(g), regarding when the data have not been obtained from the data subject.

The suitability for PIMS use also works for the objection to the profiling, in accordance with the data subjects right in Article 21. The controllers rights differs depending on the type of processing purposes. It would be very user friendly if the data subject could log onto their PIMS and simply review the controllers that used their data in profiling, and for direct marketing be able to stop the profiling immediately.[230] And for profiling under the provisions Article 6, PIMS could facilitate a line of communication between the controller and the data subject. There has also been concern regarding the possibility the data controller has to explain the logic behind highly technical systems and advanced algorithms,[231] often times the technicality and level of math required for this decision making, particularly considering big data does provide difficult challenges in explaining in a short way the logic behind the decision making. If PIMS wishes to truly be successful they should invest into making explanations in regards to automated decision making and profiling, that is understandable to the data subject. They would be dependent on receiving at least the logic behind the algorithm from the controller. While the controller might be reluctant to give the algorithm to the PIMS as this is valuable information, they could give an outline so the PIMS could explain it to the data subjects. The value of using PIMS could be highly cost saving[232] which should incentivise the controllers. While it may be difficult finding the right balance between understandable and the required detail for it to truly be explaining "the logic involved", if the controllers were

[229] Article 29 Working Party. WP 251 p. 14

[230] GDPR Article 21(2) and (3).

[231] Kuner, Svantesson, Cate, Lynskey, Millard (2017) p. 1

[232] Mydex CIC (2010) p. 22

able to use a ready-made explanation already approved by i.e. a Code of Conduct or Certification this would certainly make them more interesting to the market.

Article 22(2) lists exceptions to the rule in Article 22(1); (a) if the decision is necessary for the performance, entering into a contract between data subject and controller, (b) under authorization by Union or Member state law which still ensures the data subjects rights, freedoms and legitimate interests, or, (c) the decision is based on explicit consent. These exceptions do not apply to special categories of personal data as mentioned in Article 9(1), with some exceptions. Safeguards may be pseudonymisation, in which PIMS previously have been mentioned as a possible valuable partner. This provision will most likely be highly relevant for several controllers, as today's level of data quality and volume is unprecedented. Because of this it is likely that Member States will regulate and allowance for processing for the public good, which has been pointed out as necessary for public development and as core to the 17 Sustainable Development Goals defined by United Nations.[233]

4.8 Data protection by design and by default

Under the GDPR there are several new data subject rights, which gives new obligations for controllers and processors. One of them is data protection by design and by default, or privacy by design[234]. According to Article 25(1) the controller shall "both at the time of the determination of the means of processing and at the time of the processing itself, implement appropriate technical and organizational measures" designed to implement data -protection principles. Pseudonymisation is an example of such measures. The provisions state the controller can take into account the "state of the art, the cost of implementation and the nature, scope, context and purposes" of the processing, as well as "risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing". Which makes the provision fluid, in that it depends on the data, the controller and other factors how much is required of each controller. There therefore seems to be some possibility for circumvention of this provision, however, this will not be in accordance with the general principles of the GDPR. PIMS can be a valuable tool for compliance with the provision. The provision has been described as unclear in terms of getting the message through to the technical developers, which is a real challenge when evaluating compliance.[235] PIMS could with good data protection organisation and technical systems in place perhaps make compliance with this provision easier,

[233] Lepri, Staiano, Sangokoya, Letouzé, Nuria Oliver (2017) p. 19

[234] For this thesis we will use the terminology data protection by design and by default as Privacy by Design can have a different meaning. See Bygrave (2017)

[235] Bygrave (2017)

as each controller itself would not have to make investments into protection by design and default.

Article 25(2), states that for the controller to be compliant with law, they must themselves implement “appropriate technical and organisational measures” that ensures only the data that is necessary for the purpose is processed. Meaning PIMS as a controller need to implement features that promote data protection. Such as the Respect Network that has step-by-step solutions for the data subject to decide to what degree they want to use the PIMS, this organising of the system promotes data security as the data subject is always aware and in control of how their data is used.[236] The PIMS openPDS/SafeAnswers have this configured to be most use to the data subject, only giving out the exact information requested and effectively through technology sharing only the exact parts of data needed to perform the service.[237] Which promotes the Article 25(2) privacy by default in that it limits the “amount of personal data” sent to the controller, and it’s “accessibility”.

4.9 Data Protection Impact Assessment (Privacy Impact Assessment)

A new feature of the GDPR is the data protection impact assessment (sometimes referred to as privacy impact assessment, for this thesis we will use DPIA), requiring the controller to "carry out an assessment of the impact of the envisaged processing operations on the protection of personal data". The assessment should be done when a processing "is likely to result in a high risk to the rights and freedoms of natural persons".[238] A DPIA is mandatory for the cases listed in Article 35(3). There are exceptions and further evaluations for what kind of data is processed and what process is in question.[239] This is a process which is mainly internal for the controller, PIMS would therefore not be of much use in order to simplify the adherence to the GDPR for the controllers as the data subjects are not directly involved, other than it is their data being evaluated. And they would need to adhere to the provision for the data where they are demmed controllers. Except for in relation to Article 35(9) which states that the controller shall where "appropriate" seeks the "views of the data subject". This direct outreach to the data subject could be done by a PIMS, and compliance would be easy for the controller to document. Whether through a PIMS is an acceptable format for the controller, the WP29 states that "those views could be sought through a variety of means", amongst those they mention studies and surveys or replies from representatives.[240] A direct question to the data

[236] Respect Network FAQ (2017)

[237] Such as a model openPDS/SafeAnswers markets itself to users with

[238] GDPR Article 35(1)

[239] Article 29 Working Party. WP 248 p. 6

[240] Article 29 Working Party. WP 248 p. 13

subject through their PIMS therefore seems to satisfy any bar of "view", but this would also depend on context. If used for i.e. profiling a direct question to the data subject through their PIMS is unlikely to be viewed as insufficient context considered.

4.10 Data transfers

According to the GDPR Article 44 any data that will be processed or is being processed in a third country or any international organization falls within the scope. Including compliance with conditions for onward transfers, meaning the data is to go from the third country to yet another party. The GDPR provides provisions for onward transfers.[241] The transfer has to be compliant with the rules for processing under the GDPR, and if there is transfer to a third country or international organization the conditions in GDPR Article 44 also has to be met.

According to the GDPR Article 45 section 1, transfer of personal data can take place if the Commission has decided that the receiving end has "an adequate level of protection". The following criteria for an "adequate" level is based on EU law, in particular the case *Schrems v. Data protection Commissioner*.[242] When the Commission has deemed a country as "safe" there is no need for any further authorization. [243] The US is currently one of these safe countries with the EU-US Privacy Shield.

There is also the option of the transfer to be lawful under GDPR by "explicit" consent of the data subject as follows in GDPR Article 49(1)(a) and (3). The data subject must here be informed that the data is to be transferred to a third country or international organization and the possible risk in agreeing to this. Also, who will receive the data, and the location of the data[244] While the change in language from the Directive from "unambiguous" in Article 26(1)(a) to the need for "explicit" consent seems like a change without much practical difference, when read with the rest of the new provisions, it can be read as underlining the rest of the new provisions. The addition of the need to inform of any risk of a transfer to a third country as well as who is receiving and the location, could amount to a difficult practical change for those who rely on consent for their transfers out of the EU.[245] PIMS could be effective in an intermediary role here. While it is not easy for organizations spanning over many countries knowing what the risk for transfer at that particular country, a PIMS would need to have this information as a part of their day-to-day workings in order for it to be fully functional as an actual

[241] Voigt, von dem Bussche (2017), p. 116

[242] Case C-362/14, *Schrems v. Data protection Commissioner* paragraph 28

[243] Voigt, von dem Bussche (2017), p. 117

[244] Voigt, von dem Bussche (2017), p. 118

[245] Dr. Gabel, Hickman,. (2016)

benefit for business and organizations as well as for data subjects. This could be utilised by giving updates to the data subject regarding data security in the country their data is headed, and give them the option to retract their consent.

For those relying on consent, without the data subjects being aware of their data being transferred across the EU/EEA, should hope for a general PIMS system, such as a governmental project where all citizens have a PIMS account which any data controller could find the data subject and easily communicate, otherwise they would need to do it by themselves or use a private PIMS organisation.

5 Conclusion

PIMS offers a new way for data subjects to control their data. Today data is scattered with different providers, all with different access points and access possibilities. PIMS promise their users one place where they can store, access, review, change and more in order to regain control over their personal information. In this the examples we have reviewed are successful. An issue is connecting the PIMS with the different controllers, should the data subject but not the controller chooses to use PIMS. While this thesis showcases many different principles and provisions that are more easily upheld when utilising PIMS, gaining traction in the market will be a challenge for PIMS in regards to larger corporations as the benefits might not be enough for them to consider a user-centric approach to the degree PIMS does. However, in the small and medium sized business market PIMS will most likely grow as the reality of GDPR sets in and costs for data processing and controlling grow.[246] The benefits of using PIMS, such as gaining a trusting relationship with the consumers and facilitation of compliance also adds to the potential of making PIMS popular, in particular when considering todays distrust of the data use, exemplified with the Snowden Effect.[247]

PIMS is a privacy centred business at such a high level that facilitation of compliance with the GDPR goes hand in hand with its basic functions, and is in particular strengthened by its user centric approach, considering the GPDR has much focus on the communication with the data subject. The support this gives its users is therefore also beneficiary to the controllers, in regards to legal compliance. The user-centric privacy approach also facilitates PIMS' own compliance with the GDPR. The user-centric approach supports the PIMS themselves in that they need trust on a higher level than would a normal controller or processor, as trust is a ground pillar they cannot stand without. PIMS if utilised correctly would therefore be a good facilitator for compliance with the GDPR, as well as highly supportive of its users' data protection. PIMS different functions has proven for several principles and key provisions supportive to facilitating compliance with the GDPR.

[246] Brochot, Brunini, Eisma, Larsen, Lewis, (2015-2015) p. 11

[247] Hautala (2016)

6 Table of reference

6.1.1 Litterature

Allfiled. *News*. (2014) https://www.allfiled.com/news/ [22.11.2017]

BankId website. (2017) https://www.bankid.no/en/about-us/ [15.11.2017]

Bits About Me. *Enterprise* https://bitsabout.me/en/enterprises/ [27.11.2017]

Bought by Many. *Privacy Policy & Cookies* (2015) https://boughtbymany.com/privacy-policy/ [21.11.2017]

Brochot, Guillaume, Brunini, Julianna, Eisma, Franco, Larsen, Rebekah, Lewis, Daniel J. “Personal Data Stores” England: the University of Cambridge (2014-2015) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=10496

Bygrave, Lee A. "Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements", *Oslo Law Review02 / 2017* (Volume 1) (2017), p. 105-120.

CitizenMe. https://www.citizenme.com/public/wp/ [26.11.2017]

CitizenMe. *Terms and Privacy*. (2017)
https://www.citizenme.com/public/wp/terms-privacy/#1456424233861-2ac0544b-8934
[22.11.2017]

Cheap Energy Club (2017) https://www.moneysavingexpert.com/cheapenergyclub
[26.11.2017]

Colombus, Louis. *Internet Of Things Market To Reach $267B By 2020.* (2017),
https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#3af186f0609b

Ctrl-Shift. “Personal Information Management Services: An analysis of an emerging market. Understanding the impacts on UK businesses and the economy”. (2014)
https://www.nesta.org.uk/sites/default/files/personal_information_management_services.pdf

Ctrl-Shift. “Personal Information Management Services: An analysis of an emerging market” (2014) https://www.nesta.org.uk/sites/default/files/personal_information_management_services.pdf

Ctrl Shift. *What we do*. (2017)
https://www.ctrl-shift.co.uk/what-we-do/ [22.11.2017]

Data Protection Commissioner Ireland, *Update on litigation involving Facebook and Maximillian Schrems Explanatory Memo.* (2017)
https://www.dataprotection.ie/docs/28-9-2016-Explanatory-memo-on-litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm [23.10.2017]

de Montjoye, Yves-Alexandre, Shmueli, Erez, Wang, Samuel S, Pentland, Alex Sandy. "openPDS: Protecting the Privacy of Metadata through SafeAnswers" Plosone, July 2014 | Volume 9 | Issue 7

Department for Business, Innovation & Skills
The Rt Hon Edward Davey. *The midata vision of consumer empowerment.* (2011)
https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

Dr. Gabel, Detlev, Hickman, Tim. *Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation.* (2016)
https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection [01.11.2017]

Electronic Privacy Information Center (epic.org*). Schrems v. Data Protection Commissioner*.
https://epic.org/privacy/intl/schrems/ [25.10.2017]

European Data Protection Supervisor (EDPS), Opinion 9/2016.
https://edps.eropa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf [15.08.2017]

Evry. *The GDPR – opening up the personal data economy*. (2017)
https://www.evry.com/no/campaigns/the-gdpr--opening-up-the-personal-data-economy/
[30.11.2017]

IT Governance Privacy Team. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*, (Second edition), Ely, United Kingdom: IT Governance Publishing, (2017).

Forgó, Nikolaus, Hänold, Stefanie and Schütze, Benjamin. “The Principle of Purpose Limitation” in, *New Technology, Big Data and the Law*, Marcelo Corrales Mark Fenwick, Nikolaus Forgó (ed.), (2017), p. 17-43

Hautala, Laura. *The Snowden effect: Privacy is good for business*. (2016) https://www.cnet.com/news/the-snowden-effect-privacy-is-good-for-business-nsa-data-collection/ [22.11.2017]

Hon, Kuan W, Millard, Christopher, Walden, Ian "Who is responsible for ‘personal data’ in cloud computing?—The cloud of unknowing, Part 2" *International Data Privacy Law*, Volume 2, Issue 1, (2012), Pages 3–18

Hub of All Things (2017) https://hubofallthings.com/ [22.11.2017]

Kuner, Christopher, Svantesson, Dan Jerker B, Cate, Fred H, Lynskey, Orla, Millard, Christopher. “Machine learning with personal data: is data protection law smart enough to meet the challenge?”, *International Data Privacy Law*, Vol. 7, No. 1. (2017).

Laney, Doug. *3D Data Management: Controlling Data Volume, Velocity, and Varity*. (2001) https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

Lepri, Bruno, Staiano, Jacopo , Sangokoya, David, Letouzé, Emmanuel, and Oliver, Nuria. “The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good”, *Transparent Data Mining for Big and Small Data*. Studies in Big Data volume 32 (2017)

Lessig, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*, Basic Books, 2006. http://codev2.cc/

Maldoff, Gabe. *Top 10 operational impacts of the GDPR: Part 3 – consent*. (2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/ [25.10.2017]

Maldoff, Gabriel. *Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization*. (2016) https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/ [01.11.2017]

Midata. *Articles of Association.* (2017) https://www.midata.coop/docs/MIDATA_Statuten_20170403_English.pdf

Midata. *home page on Transparency* https://www.midata.coop/

Mydex CIC. "The Case for Personal Information Empowerment: The rise of the Personal Data Store". (2010) https://mydex.org/sites/mydex.org/files/assets/the_case_for_personal_information_empowerment__the_rise_of_the_personal_data_store__a_mydex_white_paper_september_2010_final_web.pdf

Mydex (2017): https://mydex.org/ and https://pds.mydex.org/what-personal-data-store-0 [21.11.2017]

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

UK Information Commissioner's Office on Midata. *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) https://ico.org.uk/media/about-the-ico/consultations/2013714/dbeis-energy-midata-ico-response-20170210.pdf

UK Information Commissioner's Office on Processing fairly and lawfully. *Processing personal data fairly and lawfully (Principle 1).* (2017) https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/

Transfers of personal data to third countries or international organisations, Information Commissioner's Office, (2017) https://ico.org.uk/for-organisations/data-protection re-form/overview-of-the-gdpr/transfer-of-data/ [01.11.2017]

Respect Network. (2017) https://www.respectnetwork.com/ [29.11.2017]

Respect Network FAQ (2017) https://www.respectnetwork.com/respect-faq/ [29.11.2017]

Respect Network Blog. *One-page summary of the Respect Trust Framework* (2012) https://respectnetwork.wordpress.com/respect-trust-framework/ [30.11.2017]

Trust Hub. https://www.trust-hub.com/ (2017) [30.11.2017]

Trust Hub. *Protect & Store Fact sheet.* (2016)
https://cdn2.hubspot.net/hubfs/2380850/Assets/trust_hub_factsheet_protect&store.pdf
[22.11.2017]

World Economic Forum. *Unlocking the Value of Personal Data: From Collection to Usage.* (2013)
http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

6.1.2 Laws, treaties and public body opinions/guidelines

REGULATION (EU) 2016/679 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.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Treaty on the Functioning of the European Union (TFEU) 2012

European Data Protection Supervisor (EDPS). *Opinion on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data.* Opinion 9/2016. (2016)

Advocate General Sànchez-Bordona in Case C-582/14 Opinion of 12 May 2016, ECLI:EU:C:2016:339

WP29: WP169 Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169; 16 February 2010).

WP29: WP250 Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 03/2013 on purpose limitation (WP 250; 2 April 2013)

WP29: WP223	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 8/2014 on Recent Developments on the Internet of Things (WP 223; 16 September 2014).
WP29: WP216	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 05/2014 on Anonymisation Techniques (WP 216; 10 April 2014).
WP29: WP242	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Guidelines on the right to data portability (WP 242; 13 December 2016).
WP29: WP249	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 2/2017 on data processing at work (WP 249; 8 June 2017).
WP29: WP203	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Guidelines on Personal data breach notification under Regulation 2016/679 (WP 203; 3 October 2017)
WP29: WP248	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248; 4 April 2017).

WP29: WP251	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251; 3 October 2017).

6.1.3 Judgements/Advocate General Opinions

Casenumer/parties:	Published:
Case C‑131/12 Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD), Mario Costeja González	ECLI:EU:C:2014:317
Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland Advocate General Sànchez-Bordona, Opinion of 12 May 2016,	ECLI:EU:C:2016:339
Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland	ECLI:EU:C:2016:779
Case C‑362/14 Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd,	ECLI:EU:C:2015:650
Case C-533/07 College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer	ECLI:EU:C:2009:257