verbraucherzentrale
Bundesverband

PERSONAL INFORMATION MANAGEMENT SYSTEMS (PIMS)

Opportunities, risks and requirements

19 February 2020

Editorial information

Federation of German Consumer Organisations

Team Digital and Media

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Federation of German Consumer Advice Centres and Consumer Associations

Federation of German Consumer Organisations

CONTENTS

I. SUMMARY OF CORE POSITIONS

- A legal framework is required to ensure that personal information management systems (PIMS) act **independently, without bias and with no economic interest of their own** when processing the data they manage on behalf of consumers, so that conflicts of interest can be precluded.
- This framework must comprise a concise definition of the **fiduciary duties** of PIMS towards their users. Provisions should be set out concerning the lawfulness and limitations of contractual mandates and strict requirements regarding the transparency and appropriateness of terms and conditions should be adopted. A potential formation of monopolies must be prevented and tie-in structures prohibited. In addition, rules should be put in place to govern insolvencies and dissolutions of PIMS.
- **Quality requirements** should be stipulated by law. Strict data security requirements are needed, especially regarding the quality of the encryption of data and their transmission, but also regarding appropriate anonymisation methods. PIMS should be obliged to conduct a data protection impact assessment and consult the competent data protection authorities before they take up operation. A certification combined with appropriate monitoring should be compulsory.
- The question of whether, and to what extent, PIMS should vet data users and ensure their reliability has to be addressed. And it would also be important to clarify **questions of liability**.
- Full **cooperation** of all controllers with the PIMS should be ensured. In addition, a dialogue about interoperability and portability standards and open interfaces, as well as their development, should be promoted.
- It would be desirable for PIMS to be **supported** and established by **public** institutions. Such support should always go hand in hand with strict requirements in order to ensure that PIMS are developed with a consumer-centred focus.

II. INTRODUCTION

In recent years, the idea of ‘data trusts’ has cropped up with some frequency in the public debate, for example in the context of discussions about data ownership, autonomous vehicles and electronic patient records. Data trusts are also expected to play an important role in the German government’s data strategy.

The broad idea is that this approach could simplify the processing and exchange of data without having to compromise on the protection of the personal data of data subjects. However, the understanding of the concept of data trusts and their objectives varies significantly between different stakeholders.

The Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) approaches the subject from the consumers’ point of view and thus focuses on so-called personal information management systems (PIMS).[1] The objective behind these is to make it easier for consumers to manage their data and give them more control over their (online) identity. Although these systems are primarily intended to benefit consumers by allowing them to determine how their data is used, they also entail significant risks. Therefore, vzbv takes the view that a framework should be established which governs the lawfulness and limitations of these structures, standardises their fiduciary duties, precludes conflicts of interest and provides for control and sanctioning mechanisms.[2]

This paper should be regarded as a contribution to the discussion of opportunities and risks linked to PIMS and approaches for solving problems associated with such systems. The objective is to create conditions in which PIMS can fulfil their intended purpose in the future whilst ensuring that the risks discussed below do not materialise. This could make a valuable contribution to consumer protection and help to improve people’s confidence in digitalisation.

III. WHAT IS A DATA TRUST?

The term data trust covers a variety of different concepts which are structured in very different ways and may pursue very different objectives. Examples:

In data protection law, data trusts have been an established concept in connection with data pseudonymisation for many years. “In the classic trustee model, the trustee is a legal entity outside the controller or processor acting as a ‘third party’. It is therefore a trust centre that is independent of data collection and usage in terms of location and organisation. A trustee can, for example, be entrusted with the storage of keys for the

[1] Terms such as privacy management tool (PMT), data agent or personal data space (PDS) refer to similar concepts. For the purposes of this paper, we will be using the term PIMS, because it describes the concept best and is already an established term in the debate.

[2] See Data Ethics Commission of the German Federal Government: Opinion of the Data Ethics Commission (2019), p. 133 et seq., URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf [accessed: 10/02/2020]; English language executive summary available at https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=2

re-identification of data subjects".[3] A data trust could, for instance, act as an intermediary between a company that holds raw data and another company whose task it is to conduct big data analyses based on this data. The task of the data trust would be to pseudonymise the data and to make only the pseudonymised data set available for analytical purposes. The trust will then delete the data so that it alone is in possession of the pseudonymisation key. Areas in which this model is being used successfully include medical research and biobanks.

Microsoft used the term 'data trustee' to market a service offering to privacy-conscious corporate customers.[4] When these customers subscribed to Microsoft cloud services, their data was not stored on Microsoft servers. Instead, it was stored and processed exclusively at data centres of Deutsche Telekom in Germany. This meant that the data was subject to German and European law. It also protected the data from access by US law enforcement authorities and intelligence agencies, because the arrangement meant Microsoft itself was unable to act on potential demands for disclosure.

The debate about a sound and secure legal framework for autonomous vehicles provides another example of a data trust. In order to be able to investigate potential accidents, data is required that shows whether the vehicle was being controlled by the autonomous drive mode or by the driver and whether there were any technical defects. Storing this data solely in the vehicle or on back-end servers of the manufacturer would not be helpful. In any dispute about whether a human or the system was in control of the vehicle, the manufacturer would be a party to the dispute and, as such, must not be allowed to access the drive mode data. vzbv therefore supports the concept of storing drive mode data in the vehicle, with a back-up copy being stored by a public or state-authorised entity under a statutory framework.[5] [6]

PIMS, however, take a different approach.

IV. WHAT ARE PIMS?

PIMS can be described as a subset of data trusts. However, their focus differs from that of the aforementioned concepts and it is therefore important to differentiate clearly between them.

A key part of the background to this topic is the long-standing controversy about consent in the context of data protection law. In light of the complexity of the

[3] Data Protection Focus Group of the 2019 Digital Summit: Draft for a Code of Conduct on the use of GDPR-compliant pseudonymisation (2019), p. 16, URL: https://www.gdd.de/downloads/aktuelles/whitepaper/Data_Protection_Focus_Group-Draft_CoC_Pseudonymisation_V1.0.pdf [accessed: 10/02/2020].

[4] This service was discontinued in 2018 https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/

[5] See Verbraucherzentrale Bundesverband: Rechtssicher fahren mit automatisierten Fahrzeugen [*vzbv: Legal certainty for travel in autonomous vehicles*] (2017), p. 14, URL: https://www.vzbv.de/sites/default/files/downloads/2017/03/21/2016-12-30_stn_zum_gesetzentwurf_aend_stvg_neu.pdf [available in German only; accessed: 10/02/2019]

[6] See joint letter by the ADAC, VdTÜV, GDV and vzbv addressed to Andreas Scheuer, Federal Minister of Transport and Digital Infrastructure, dated 16 July 2019, on the storage location of drive mode data pursuant to § 63a of the German Road Traffic Act (StVG)

technologies and business models involved nowadays, it has become almost impossible for consumers to make properly informed decisions about consenting to the processing of their personal data. It can also be difficult for data subjects to keep track of the companies to which they may have given consent for data processing in the past, with implications for their ability to potentially withdraw their consent at a later stage. This is where PIMS come in.

> PIMS are “new technologies and ecosystems which aim to empower individuals to control the collection and sharing of their personal data.”[7] The central idea of this concept is to put the individual consumer at the heart of the data management process and to enable them to take control of their (online) identity.[8]

Back in September 2016, the European Data Protection Supervisor published an opinion discussing how PIMS could play a role in improving personal data protection and what challenges this might entail.[9] The European Commission also published a report in November 2016 in which it examined the opportunities and risks associated with PIMS.[10] And quite recently, the Data Ethics Commission of the German government (DEK) also highlighted the benefits and risks of PIMS.[11]

There are currently a number of PIMS concepts[12] that differ substantially from one another in terms of their objective, business model, reach (industry-specific or universal) and technical and organisational design.[13] In addition, many of these concepts are not yet very mature. Consequently, there are huge differences in terms of their potential benefits, the scale of the associated risks and the resulting need for regulation. The aspects discussed in the following chapters thus do not necessarily apply to all PIMS and are primarily intended as an initial overview of this extensive field.

---

[7] European Data Protection Supervisor: EDPS Opinion on Personal Information Management Systems. Opinion 9/2016 (2016), p. 5, URL: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf [accessed: 10/02/2020].

[8] This idea does not apply to the concepts described above

[9] European Data Protection Supervisor (EDPS) (2016) (as footnote 7 above).

[10] European Commission: An emerging offer of “personal information management services” (2016), URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118 [accessed: 10/02/2020].

[11] Data Ethics Commission of the German Federal Government (DEK) (2019) (as footnote 3 above), p. 133 et seq.

[12] See Foundation for Data Protection: New ways of providing consent in data protection - technical, legal and economic challenges; study (2017), p. 20 et seq. URL: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf [accessed: 10/02/2020]; English language summary available at https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_PolicyPaper_New_ways_of_providing_consent_in_data_protection_EN_final.pdf.

[13] Differences could, for instance, relate to the following aspects: Is data stored locally on the data subject’s device or in the cloud? If access to data from various different sources is intended, is such data stored within the PIMS or does the data remain at its source location and the PIMS merely establishes a type of ‘link’? Do prospective data users have direct access to the data, or is the data analysed within the PIMS (subject to restrictions that may be imposed by the PIMS), or does the PIMS conduct the analysis itself with only the results being made available to the data user? See Blankertz, Aline: Designing Data Trusts (2020), p. 20 et seq.; URL: https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_d.pdf [accessed: 18/02/2020].

1. WHAT ARE THE POTENTIAL BENEFITS OF PIMS?

Broadly speaking, the hope is that PIMS will help to enable consumers to exercise their right to personal data protection more actively in a world that is becoming ever more complex.

A key element of PIMS is usually the concept of **consent management**, which allows consumers to specify in one centralised place how their personal data may be processed, by whom and for what purposes. For example, consumers could use the PIMS to make their data available for scientific research or for commercial purposes. By centralising the consent management and the associated documentation of all instances in which consent was given, it becomes easier for consumers to maintain an overview of their data and the processing activities performed by the various data users. A functionality that allows consumers to set **data protection preferences** and to apply and/or change these for multiple providers at the same time would significantly reduce the amount of effort involved in consent management. Another beneficial feature could be that consumers would no longer need to consent to a whole host of potential processing purposes upon every initial interaction with a new service provider. Instead, the service providers could simply request the consumer's consent when they want to perform a specific type of data processing. This would also allow for more granular consent management than currently practised. In addition, it would be possible to implement technical features that allow consumers to grant consent for a limited period of time only.

Further-reaching concepts envisage a possibility for consumers to define data protection preferences that are then executed by artificial intelligence (AI) tools, creating a **dynamic consent** system. This could, for instance, apply in a case where a consumer specifies that they generally want to make their data available for medical cancer research conducted by public institutions, but not for any other purposes nor to any other type of organisation. If a suitable research institution is interested in the data, the consumer could be contacted through the PIMS in relation to this specific use case with a request for consent and relevant case-specific information.

PIMS are also intended to improve **transparency**, which is a prerequisite for informed consent management. One idea is to use the requests from processors to generate standardised declarations of consent that are easy to understand for consumers. If the general privacy policy of a company is machine-readable, the PIMS could 'translate' it into a single-page summary or a graphic or icons based on the relevant preferences set by the consumer.

In an ideal scenario, PIMS would also be able to ensure (by means of cryptographic processes or, less preferably, through contractual agreements) that the data made available can definitely be **used for none other than the specified purposes** (and, of course, by authorised entities only). In addition, individual incidents of data access could be logged and thus made traceable.

Other approaches include the development of PIMS into a central platform that offers functionalities for exercising **further data protection rights** such as the right of access and the right to data portability. Consumers could, for instance, send requests for information about or transfers of their data to companies through the PIMS, and the recipient companies could send an automated response using dedicated technical interfaces. This would make it easier for consumers to exercise their rights and would also help companies to optimise their processes. Similar mechanisms could apply for the right to erasure, the right to rectification, the right to object, etc.

Some participants in the current debate also propose that PIMS should include a **pseudonymisation function**. This means that if such a PIMS received an age verification request, for example, it would not reveal the actual date of birth of the consumer but would simply confirm whether or not the consumer meets the relevant age threshold. **Data anonymisation** could also be a PIMS function, for example to make data more easily accessible for research purposes and to minimise privacy risks.

The extent to which consumers could be enabled to **use PIMS to have their data analysed for their own purposes** is also a point of discussion. Consumers who have made their data available for medical research, for example, could be provided with visualisation and analytical tools that might help them to improve their own health. The development of privacy-enhanced digital assistants based on the data sets stored in PIMS would also be conceivable.

However, PIMS are intended to benefit not only consumers but also companies. The aim of improving the consumers' level of control is to strengthen their **trust and confidence** in digitalisation and the data processing industry. This would make it easier for companies to **make data usable**. Another benefit for companies would be access to data pools of higher **quality**, which – in turn – could improve the quality of data analysis and research. Last but not least, companies would enjoy greater **legal certainty** in relation to data protection, because it would, for instance, be easier to obtain consent in a manner compliant with GDPR requirements.

2. WHAT ARE THE POTENTIAL RISKS OF PIMS?

Although these systems are primarily intended to benefit consumers by allowing them to determine how their data is used, they can also entail significant risks. The DEK, for example, points out that consumers could be led to surrender more and more control to others without being aware of or concerned about this shift. Scenarios where data subjects transfer a significant portion of their decision-making rights to the system operators, or where operators unduly influence the decisions of data subjects against the data subjects' best interest, would run counter to the core idea of PIMS.[14]

This means that PIMS have to satisfy two customer groups – data providers and data users – that have different interests. The **company and business model selected** by a PIMS plays a key part in this context. If, for example, its funding model is based on an access fee payable by prospective data users, the PIMS will have an interest in encouraging the consumers who supply the data to store as much data as possible in the PIMS and to make this data available. On the other hand, PIMS would probably find it difficult to attract a large number of consumers to use their services if they had to pay for it. In addition, one of the core concepts of the PIMS is to improve the protection of private individuals' personal data. Making access to these services contingent on purchasing power would thus be problematic. For private sector PIMS, the key challenge will be to develop a viable business model that neither compromises the all-important trust of consumers nor contradicts its inherent purpose.

In addition, **conflicts of interest** could arise between the PIMS and the consumers that use them, depending in part on the corporate structure of the relevant system. The service provider Verimi is a case in point: Its shareholders include companies like

[14] See Data Ethics Commission of the German Federal Government (DEK) (2019) (as footnote 3 above), p. 133.

Allianz, Axel Springer, the Bundesdruckerei (German Federal Printing Office), Daimler, Deutsche Bahn, Deutsche Bank, Deutsche Telekom, Lufthansa, Samsung and Volkswagen Financial Services. In its early days, this service was advertised to consumers as a privacy-enhanced alternative to the single sign-on services offered by Facebook and Google and as a consent management service. However, within the advertising industry, the services was regarded as a means of guarding against the stricter consent requirements for online tracking to be introduced by the upcoming e-privacy regulation.[15] According to comments by Verimi employees published in the press, this approach was abandoned.[16] But this example highlights potential risks.

There is also a risk that products could be presented as PIMS acting in the interest of consumers, although they are **essentially B2B applications**. This would, for instance, be the case if companies wanted to exchange data but required consent from the data subjects as personal data would be involved. The Neutral Extended Vehicle for Advanced Data Access ('NEVADA') system operated by the German automotive sector is a fitting example. Data generated by vehicles is stored on a 'neutral server' and can then be made available to other companies.[17] The idea is that the customer can determine which third parties will be able to access the data. vzbv opposes the formation of information monopolies held by a small number of companies and thrives to protect fair competition. It therefore opposes any model that involves data being stored on manufacturers' back-end servers. A free choice for consumers between different providers can only be guaranteed if manufacturers do not have first access to vehicle data. Decentralised storage is therefore preferable from a consumer perspective.[18]

Another common argument is that PIMS could be an instrument that enables consumers to **monetarise their data**. In debates about "data ownership", "data trusts" (here in the sense of PIMS) were proposed as a type of **collective rights management society** for personal data. In a scenario where some form of data ownership is introduced, consumers should have the option to transfer their ownership rights to a "data trust". Advocates of this approach argue that this would mitigate the power asymmetry in the negotiating positions of consumers and companies, since the data trust would exercise quasi-proprietary collective data usage rights.[19] However, for

[15] Günther, Vera: Datenschutz und Datenallianzen [*Data protection and data alliances*]; in: Horizont (2018), URL: https://www.horizont.net/medien/nachrichten/Datenschutz-und-Datenallianzen-Wenn-wir-nicht-reagieren-fliessen-noch-mehr-Gelder-nach-Amerika-164094 [available in German only; accessed: 10/02/2020].

[16] Bröckling, Marie: Eine Identität für alles: Das schwierige Geschäftsmodell von Verimi [*One identity for all occasions: The controversial business model of Verimi*]; in: Netzpolitik.org (2018), URL: https://netzpolitik.org/2018/eine-identitaet-fuer-alles-das-schwierige-geschaeftsmodell-von-verimi/ [available in German only; accessed: 10/02/2020].

[17] See German Association of the Automotive Industry (VDA): Data security for networked mobility (2017), URL: https://www.vda.de/en/topics/innovation-and-technology/data-security/what-is.html [accessed: 10/02/2020]

[18] See Jungbluth, Marion: Wird das automatisierte und vernetzte Fahrzeug zur digitalen Zwangsjacke für Verbraucher? [*Will autonomous networked vehicles become digital fetters for consumers?*] Published in: Alexander Rossnagel, Gerrit Hornung (editor): Grundrechtsschutz im Smart Car [*Protection of fundamental rights in the context of smart cars*] (2019), pp. 381–397

[19] See Jöns, Johanna: Daten als Handelsware [*Data as a tradable good*] (2016), pp. 12, 74, 85, URL: https://www.divsi.de/wp-content/uploads/2016/03/Daten-als-Handelsware.pdf [available in German only; accessed: 10/02/2020].

a number of reasons, vzbv has decided to oppose data ownership and, consequently, data trusts in this form and context.[20]

The monetisation of personal data poses a risk that extends beyond discussions about data ownership and could be exacerbated by the establishment of PIMS. The service provider Weople, for instance, represents its users towards various services and platforms and collectively exercises their right to data portability on their behalf. Weople then commercialises the data that has been transferred to it and passes a share of the profit on to its users.[21] However, offering consumers direct **financial compensation** for the processing of their data is highly problematic. Reducing the status of personal data to that of a financial asset is unacceptable from a fundamental rights perspective. Offering consumers direct financial compensation in exchange for the commercialisation of their data creates detrimental incentives, especially for low-income population groups. Rather than solving existing issues in the data industry, such models just create additional problems.

There are further problems that need to be taken into account in the development and operation of PIMS. For example, service providers need to ensure that their **data security** is top notch as they could be an attractive target for attackers – especially if their data is stored in a centrally. They also need to ensure that the data made available to data users through their service will be processed in strict accordance with the consumers' preferences and the **agreed purposes**. In addition, the rights of consumers could be compromised if a PIMS is **taken over by another company**.

3. WHAT REQUIREMENTS SHOULD APPLY TO PIMS?

In order to address the aforementioned risks, a **framework providing legal certainty** for PIMS should be developed. This framework should go beyond the GDPR in some respects and further clarify it in others. Ideally, it should be implemented in the form of legislation at European level. To some extent, these requirements can also be applied to other types of data trust.

The legal framework is required in order to ensure that PIMS act **independently, without bias and with no economic interest of their own** when processing the data they manage on behalf of consumers and that conflicts of interest are precluded. In this context, it is of particular importance to ensure that the role of the PIMS as a trustee is not undermined by commercial motivations. Financial and other interest-driven interdependencies between PIMS and other private-sector entities must also be precluded. vzbv would regard it as preferable for these types of structures to be operated by foundations or public institutions, but private-sector models would also be conceivable, if fiduciary duties are imposed, quality requirements defined and liability-related issues clarified.

The **fiduciary duties** of PIMS towards their trustors, i.e. the consumers, must be set out very precisely. For instance, rules regarding the lawfulness and limitations of

[20] Verbraucherzentrale Bundesverband: Rechte an Daten. Kurzpapier des vzbv [*vzbv: Rights to data; summary paper*] (2018), URL: https://www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-26_vzbv_rechte-an-daten_kurzpapier_final.pdf [available in German only; accessed: 10/02/2020].

[21] Pappalardo, Massimiliano: Data for money: App facilitating data portability now under the EDPB's scrutiny (2019), URL: https://iapp.org/news/a/data-for-money-app-facilitating-dsars-now-under-the-edpbs-scrutiny/ [accessed: 10/02/2020].

contractual mandates would be required, especially if PIMS exercise consumers' rights under the GDPR (e.g. granting and withdrawing consent, right of access, right to erasure, right to data portability, etc.) on their behalf. PIMS should also be required to comply with very strict requirements regarding the transparency and appropriateness of their terms and conditions. In addition, it must be ensured that data processing by default is excluded. Last but not least, monopolies must be prevented from forming and tie-in structures prohibited in order to ensure that providers cannot, for instance, force their customers to use a particular data trust. Provisions on how to handle the insolvency or dissolution of a PIMS would also be important.

As data subjects are very limited in their ability to assess the quality and reliability of a PIMS, certain **quality requirements** should be prescribed by law. Strict data security requirements should be developed, especially regarding the quality of the encryption and transmission of data, but also regarding anonymisation methods. Provisions obliging PIMS to consult the competent data protection authorities and conduct a data protection impact assessment before taking up operation would also be required. In addition, a certification combined with appropriate supervision should be compulsory in order to prove that PIMS comply with all applicable requirements from both an organisational and a technical point of view.

The extent to which PIMS should vet data users and ensure their reliability could also be discussed. In this context, it would moreover be important for **aspects of liability** (beyond the potential responsibility of processors) to be regulated by law. For example, clarification is needed in respect of the extent to which a PIMS could also be held liable if a data user violates data protection requirements. Compulsory liability insurance in respect of claims for damages by data subjects could be a conceivable option. The extent to which PIMS are able to contractually limit their liability towards consumers would also need to be clarified.

But above and beyond the limitation of risks, a framework providing legal certainty is also important in order to ensure that PIMS unlock the desired benefits. For example, full **cooperation** of all controllers must be ensured. As cooperation may not always be in the interest of all parties involved, the option of obliging controllers by law to cooperate with PIMS should be considered. In addition, a dialogue about **interoperability and portability standards and open interfaces** and their development should be promoted.

It would generally be desirable for PIMS to be **supported** and established by **public** institutions. However, such support should always go hand in hand with strict requirements in order to ensure that PIMS are developed with a consumer-centred focus. In future, PIMS could also be used more widely as an interface for citizens' affairs and it might therefore make sense for public institutions to impose the aforementioned PIMS requirements in such cases, in order to ensure that PIMS are fit for this type of use.