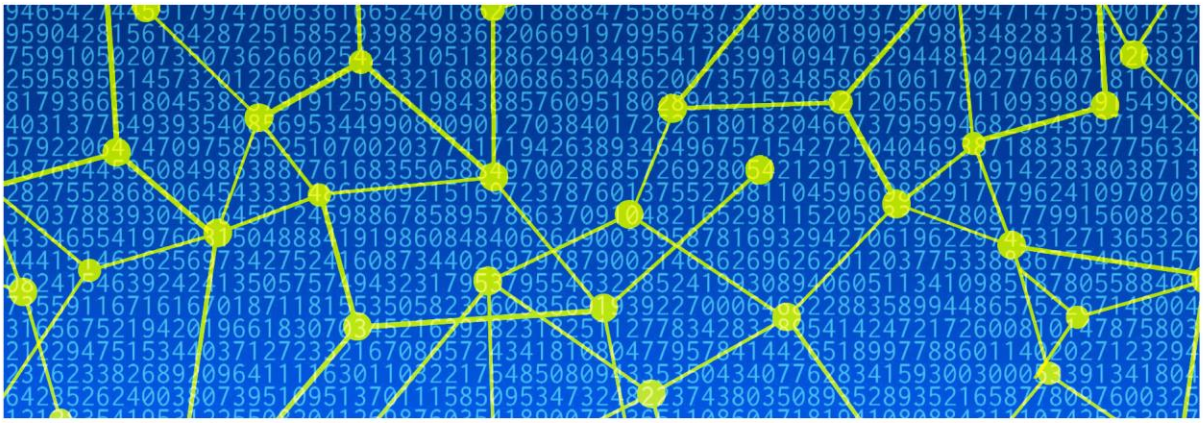

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 9/2016

EDPS Opinion on Personal Information Management Systems

Towards more user empowerment in managing and processing personal data

20 October 2016

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'with respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '… for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. The EDPS considers that the emerging landscape of Personal Information Management Systems (PIMS), aiming at putting back individuals and consumers in control of their personal data, deserves consideration with a view to contributing to a sustainable and ethical use of big data and to the effective implementation of the principles of the recently adopted General Data Protection Regulation (GDPR).

Executive Summary

This Opinion explores the concept of technologies and ecosystems aiming at empowering individuals to control the sharing of their personal data ('personal information management systems' or 'PIMS' for short).

Our vision is to create a new reality where individuals manage and control their online identity. Our aim to transform the current provider centric system into a human centric system where individuals are protected against unlawful processing of their data and against intrusive tracking and profiling techniques that aim at circumventing key data protection principles.

This new reality will be facilitated by the modernised EU regulatory framework and the possibilities offered by vigorous joined-up enforcement by all relevant supervisory and regulatory authorities.

The recently adopted General Data Protection Regulation (GDPR) strengthens and modernises the regulatory framework so that it remains effective in the era of big data by strengthening individuals' trust and confidence online and in the Digital Single Market. The new rules, including those on increased transparency and powerful rights of access and data portability, serve to allow users more control over their data, and may also help contribute to more efficient markets for personal data, to the benefit of consumers and businesses.

Most recently we have issued an Opinion on effective enforcement of fundamental rights in the age of big data. This highlights current market conditions and business practices that create obstacles for effective exercise of individuals' rights to the protection of their personal data and other fundamental rights, and calls for stepping up concerted and consistent enforcement of competition, consumer protection and data protection laws. We hope that this increased enforcement will serve to create market conditions in which privacy-friendly services can thrive. The approach in this Opinion aims at strengthening fundamental rights in our digital world at the same time as opening new opportunities for businesses to develop innovative personal data based services built on mutual trust. PIMS promise to offer not only a new technical architecture and organisation for data management, but also trust frameworks and, as a result, alternative business models for collecting and processing personal data in the era of big data, in a manner more respectful of European data protection law.

In this Opinion, we briefly describe what PIMS are, what problems they are intended to solve, and how. We then analyse how they can contribute to a better protection of personal data and what challenges they face. Finally, we identify ways forward to build upon the opportunities they offer. For new data protection business models to thrive, additional incentives for the service providers offering them may be necessary. It should be explored, in particular, which policy initiatives could motivate data controllers to accept this way of data provision. Furthermore, an initiative by public services to accept PIMS as a data source instead of direct data collection could add critical mass to the acceptance of PIMS.

The emerging landscape of PIMS, aiming at putting individuals and consumers back in control of their personal data, deserves consideration, support and further research with a view to contributing to a sustainable and ethical use of big data and to the effective implementation of the principles of the recently adopted GDPR.

TABLE OF CONTENTS

1. PIMS: SHARING DATA, SHARING BENEFITS?

1 Current conditions for the processing of personal data are often unfair to the individuals whose data are processed. Legal conditions and technical tools make it difficult for individuals to exercise their rights and allow controllers to limit their liability. Data brokers, advertising networks, social network providers and other corporate actors have ever more complete files on individuals participating in today's digital society, and individuals are losing control over the digital footprints they leave behind. Targeted, profiled and assessed by actors often beyond their control or even knowledge, individuals may feel helpless and need to be empowered to take control of their identity. Even where formally having been given some form of a 'notice' and opportunity to 'consent' to general terms and conditions, individuals often find themselves inside a system designed to maximise the monetisation of personal data, which leaves no real choice or control to individuals.

2 The European Commission's communication on big data[1] sets out a plan of actions jointly aiming at personal data and consumer protection. This specifically encourages the use of 'personal data spaces' as user-centric, safe and secure places to store and possibly allow others to access personal data. We share the view that innovative digital tools and business models based on the empowerment of individuals should be encouraged. These may allow individuals to benefit from such data-sharing, that is to participate in the use and distribution of their personal information.

3 In our Opinion on 'Meeting the challenges of big data'[2] we argued that we should complement the legal obligation of effective consent with real, practical control over personal information. We argued that '*instead of an administrative burden, providing access rights may become a feature of the service provided to the customers*', and that organisations based on exploiting 'big data' should '*be prepared to share the wealth created by the processing of personal data with those individuals whose data they process*'. In that context we noted that '*personal data stores could help address some of the concerns over the loss of individual control over personal data*'. The recently adopted General Data Protection Regulation (GDPR)[3] has strengthened the legal requirements for consent[4] and has introduced effective, modern principles of data protection by design and by default[5], as well as a new right to data portability[6]. In order for the new framework for data protection to deliver its promise we need practical tools to enable individuals to exercise their rights in a convenient, user-friendly way.

4 This Opinion explores new technologies and ecosystems which aim to empower individuals to control the collection and sharing of their personal data. We will refer to this concept as 'personal information management system' ('PIMS')[7]. The PIMS concept offers a new approach by which individuals are the holders of their own personal information. It may create a paradigm shift in personal data management and processing, with social and economic consequences. In contrast, the current landscape of online services is characterised by a small number of service providers that dominate the market by monetising users' personal data in exchange for 'free' services. This is often accompanied by an imbalance of power, where the customer is left with a 'take it or leave it' approach, and by information asymmetry between service providers and users, with little or no transparency for the individuals on what is going on with their personal data.

5 The core idea behind the PIMS concept is to transform the current provider centric system into a system centred on individuals able to manage and control their online identity[8]. In principle, individuals should be able to decide whether and with whom to share their personal information, for what purposes, for how long, and to keep track of them and decide

to take them back when so wished. It is worth exploring how PIMS could help address some of the concerns over the loss of individual control over personal data that have been highlighted as one of the key concerns about big data[9].

6 This approach aims at strengthening fundamental rights in our digital world at the same time as opening new opportunities for businesses to develop innovative personal data based services built on mutual trust. PIMS promise to offer a new technical architecture and organisation for data management which build trust frameworks. They hope to enable alternative business models for collecting and processing personal data in the era of big data, which do so in a manner more respectful of European data protection law.

7 In this Opinion, we briefly describe what PIMS are, what problems they are intended to solve and how[10]. We analyse how they can contribute to a better protection of personal data and what challenges they face. Finally, we identify ways forward to build upon the opportunities they offer.

2. MODELS AND FEATURES OF EMERGING PIMS

2.1. Architecture and technology

8 PIMS are at an early stage of development. The way they are designed and the underlying business models differ widely. There is little experience of their practical use and impact on the processing of personal information. This Section explains some of the models and features of emerging PIMS.

Where are the data?

9 A main distinction between the various types of emerging PIMS can be made on their technical architecture, whether based on local storage or cloud-based storage. In the local storage model, personal data are kept in user devices such as a laptops, smartphones, tablets etc. In the cloud-based model, users' data are mainly kept by service providers (social networks, online office suites, healthcare providers etc.) as well as by specialised cloud-based PIMS providers.

10 In the cloud-based configuration, there are two kinds of basic approaches which can also co-exist with each other. Some PIMS are designed to keep the users' data in a single place; others are creating a logical link among users' data, which may stay with various service providers.

How are data processed?

11 Data either do not leave the PIMS (and in certain models algorithms are even imported and computed internally) or data are securely transferred to the service providers, where they may also be stored in an encrypted form for the processing operations. Data and their properties are kept in an interoperable machine-readable format enabling interactions without human intervention.

How are security and data protection implemented?

12 Security and data protection are the main drivers of PIMS. Cryptography plays a fundamental role and is a necessary component for the security of the data and for mutual reliance on the authenticity and integrity of data and processing among all stakeholders in the data processing chain:

a) encryption can ensure confidentiality of data at rest and in transit;

b) cryptographic features may be used to verify the authenticity of data and to implement users' privacy preferences such as authorised purposes and permitted retention periods against service providers and third parties.

13 In some models, third parties (public or private entities) enter as new actors in the data management ecosystems as trust service providers. Their role is providing mutual trust mainly between users and service providers, by being identity providers and custodians, facilitating authorisation mechanisms and enabling the traceability of personal data and of operations performed on them.

14 Data minimisation and anonymisation services are also provided. For example, it may be possible to make a transaction where the authorisation is not subject to a complete identity disclosure (e.g. the PIMS may confirm that a user meets age requirements, instead of demanding the name and date of birth)[11]. In other cases PIMS offer anonymity[12] services vis-a-vis service providers and other parties using the data by e.g. aggregating data before they are transferred to those parties[13].

2.2. Main features facilitating control of individuals over their personal data

15 One of the main objectives of PIMS is to let users define at a sufficiently granular level how their personal information should be used and for what purposes, and enable them to keep track of the way this information is used so as to be sure that it is not processed in a way not permitted by them. It implies a comprehensive consent management functionality enabling users also to withdraw their consent when desired. Usually a user-friendly control dashboard is provided for this purpose. The other parties (other users and service providers) are usually able to access the data in an automated way according to the privacy preferences established.

16 Beyond identification, authorisation and privacy preferences management, PIMS often provide additional value added services. Some PIMS offer the possibility to retrieve data about the user's on-line presence (such as browsing history, bookmarks, address books, credentials, location data, financial data, social network activity), and organise it in the PIMS.

17 An interesting development of PIMS is the possibility of including personal analytics features. This would support the new paradigm where users are in control of their data and what the data say about them. In a hypothetical world where all information relating to a user is available to him or her, the user could have a privacy-friendly personal assistant controlling how information from their personal 'big-data' repository is used. This could be done in a sector specific context (e.g. well-being and health data, personal mobility) or in a holistic perspective where data collected about an individual from different sources and in various contexts are aggregated. Users would control how their personal information and/or insights inferred from it are shared with external parties, according to their preferences and for mutual benefit.

2.3. PIMS policy framework and business models

18 PIMS require more than a new data management architecture based on adequate technology. In addition, a commonly agreed policy, trust in its implementation, and mechanisms to monitor and verify this trust and remediate when things go wrong, are also

essential, to ensure effective security and data protection in a self-regulated environment building upon the legal framework.

19 As a result, some organisations[14] propose PIMS where the secure and privacy friendly management of personal data is ensured by the contribution of many actors, with different roles, under a policy to abide by and a governance scheme. The idea is to create new communities of trust based on transparency and fairness, where traditional online service providers, new economic operators (e.g. PIMS service providers and trust providers) and the individuals whose personal data are managed and processed, can each take a fair share of the benefits of big data.

20 Current prevailing business models for PIMS providers (and other actors enabling the whole ecosystem) are based on online service providers and third parties paying fees or sharing revenues to use the PIMS schema/services. Individuals would in general enjoy free PIMS services, with some possible exceptions for extra services directly provided by the PIMS operator or their business partners.

3. HOW PIMS CAN SUPPORT DATA PROTECTION PRINCIPLES

21 PIMS face significant challenges to become mainstream for personal data management in a market dominated by a small number of operators that may often not be interested in creating synergies with them[15]. None the less, PIMS deserve support and investment in so far as they may support many of the data protection principles, tools and safeguards that are at the core of the new GDPR.

22 Support is essential to those PIMS that genuinely are striving to deploy solutions compliant with the EU data protection vision and legal framework. This would have to be hand-in-hand with effective enforcement of the legal safeguards protecting users against unlawful processing of their data and intrusive tracking and profiling techniques that aim at circumventing key data protection principles.

23 In the following Sections we examine these principles, tools and safeguards and consider the challenges to be addressed.

24 Issues to be explored include: how data protection principles are actually implemented (e.g. data subjects' rights, mechanisms for valid consent, controllership and liability, data protection by design, security); interoperability and technical feasibility; business models and interests at stake in PIMS; and the ownership of personal data in the PIMS context.

3.1 Effective consent management to ensure genuine user control and the use of automated mechanisms

25 Consent management is the core function of PIMS, implementing an automated matching of user preferences with requests for personal data. It is essential that privacy preferences are expressed with sufficient granularity and take into consideration a complex context of possible options. Furthermore, especially where the nature of the data and the type of processing could entail high risks for the individuals, their contextual awareness should be raised and mechanisms to trigger human intervention should be available in the PIMS. It could be explored whether it can make sense, and under what safeguards and conditions, to express consent for broader, wider contexts such as medical research sectors.

26 It is also important that these automated mechanisms should be periodically matched against the real current will of the individual through *ad hoc* reminders, to avoid risks arising due to the inability (whatever the reason) of individuals to change their preferences.

27 The use of machine-readable forms of expression of privacy preferences, which either travel with the data (often called 'sticky policies') or logically link with the data, and of protocols enabling their exchange has not entered the market yet and needs further investments to break into real life applications. Several projects have focused on this in the past[16], and other developments have followed[17] that deserve attention and further analysis for possible support.

28 In particular, valid consent needs to be informed[18]. Trust frameworks regulating the use of PIMS by individuals and other stakeholders (see Section 2.3) mandate transparency and information. It is also to be noted that notwithstanding the research efforts relating to the use of machine readable privacy policies, in certain circumstances, individuals will need still to rely on their human assessment to verify the level and the adequacy of the information provided.

3.2 Users in control, rights to access and rectification, right to data portability, data quality

29 The main objective of PIMS is to put users in control of their personal information. In addition to serving as an effective and user-friendly mechanism to provide or withdraw consent, well-designed PIMS would also facilitate the users' rights of access to their data and their right to keep it up-to-date and accurate, thus enhancing the quality of data. PIMS are among the most promising efforts to implement by design the right to access and rectification and the new right to data portability[19]. They could also improve accuracy of the data[20] and ensure use limited in time, thus facilitating compliance with the storage limitation principle[21].

30 While most if not all existing PIMS share these objectives and have features to meet them, this does not necessarily mean that risks of loss of confidentiality and unfair use of the data completely disappear. Technical measures may help discover and provide proof of what went wrong, but if data leave a PIMS in unencrypted form, or even if data are lawfully obtained but subsequently decrypted by an organisation that does not comply with its obligations, there is a risk that data will be accessed and used differently from their permitted use configured in the PIMS. This calls for caution and verification of what the PIMS are advertised to do against the reality.

31 The user-friendliness of PIMS and the ability of users to obtain the desired effects by using them is also of outstanding importance, in particular if confronted with the risks of exposing personal data, including sensitive data, to automated consumption by online services. PIMS services should be complemented by extensive educational material and step-by-step guidance and training, notwithstanding the intended ease of use. Providers and developers should consider prospective use by the general public, who are not necessarily equipped with technical and data protection skills and knowledge.

3.3 Data protection by design and by default, interoperability

32 Online service providers, acting as controllers when offering their services, could be supported in complying with the obligation of data protection by design and by default by enabling their services to interface with EU data protection compliant PIMS, and allowing

that users' personal data could easily and conveniently be exported to the individual's PIMS. Collecting and managing the user's consent, transparency and accountability, security when exchanging data, as well as authorisation mechanisms would need to rely on the features of the PIMS. This means that the responsibility of PIMS operators in designing them in compliance with the GDPR is a fundamental issue. Therefore, policy makers should support PIMS in designing their services specifically with the objective of facilitating compliance with the GDPR.

33 Interoperability is a crucial requirement, which has to be addressed by PIMS[22]. More standardisation efforts are needed by the emerging PIMS industry and these efforts should be facilitated by policy makers.

3.4 Technical means to restrict further use of personal data

34 The enforcement of consent and purpose specification/limitation and data retention to automate matching individual preferences with the online offer (Section 3.1) relies on mutual trust and a-posteriori verification if no adequate technical safeguards are in place. As already mentioned above, solutions have been found[23] that make sure that those rules are automatically verified and enforced, preventing access to the data themselves if rules are not complied with. Cryptography supports the verification of the identity of the data consumer, the match against the permitted and the declared purposes, and guarantees the integrity of the data and of the parameters used to keep control. When, for example, an online service provider wants to use personal data, which are exchanged in an encrypted form, for purposes different from those authorised by the individual, the unavailability of the relevant decryption keys will prevent the access[24].

35 Keeping control of personal data in the era of the Internet of Things and Big Data cannot succeed without an automated and reliable, yet controlled, enforcement of data protection rules. We believe this is one of the critical areas where research and investment effort should focus.

3.5 Transparency and traceability

36 Not all personal data processing is legally based on consent. For example, eGovernment applications are more likely to be based on specific EU or national legislation or on another legal basis such as necessity for carrying out a task in the public interest[25]. Even in these cases PIMSs features to control how data can be very useful to enhance transparency and traceability. PIMS could indeed facilitate informing citizens about transfers in accordance with the applicable data protection legislation. For example, by looking at their dashboard in their PIMS citizens could know whether their personal data have been transferred between two different public administrations in cases where transfers are defined by law. Furthermore, even where data is processed for a specific purpose based on another legal basis, PIMS can help individuals to effectively manage their consent for possible further utilisation for other purposes. In such cases mechanisms informing and warning the individual of a possible change of purpose should be designed to facilitate compliance with data protection principles.

3.6 Data security

37 Identification and authorisation mechanisms in PIMS can benefit from research and developments in other contexts. Open and scalable identification, authentication and

authorisation architectures and solutions are already in use and initiatives are on-going to improve the technology. Data minimisation can be based on the fact that authentication is different from identification: an individual does not necessarily need to identify himself or herself to be granted authorisation to access and use a resource; instead, it is sufficient to show a valid authorisation (whose 'validity' is e.g. mutually ensured by a mutually trusted third party).

38 A high level of security is one of the features required by PIMS. As mentioned, here the architecture and the use of encryption make the difference. Strong, secure encryption should always be an essential component of PIMS to deliver on their promises. As to encryption, key management is one of the determining factors. Different models are proposed, ranging from keeping the encryption keys locally by an individual's device, or by the PIMS provider or by a trusted third party. All of them have different risks and opportunities. In any case the physical separation of keys and data is highly recommended. Centralised storage of all or a very significant portion of a user's personal data might represent a high risk per se. As to key storage location, many security experts agree that it can be risky to store data locally in personal devices because they often feature a low level of protection. On the other hand, cloud-based services bear also their own specific security risks. In many circumstances, though, entrusting individuals' own data to a trustworthy PIMS operating in a secure and well-designed cloud-based environment could be a sustainable choice.

39 PIMS should be clear towards customers on the benefits and risks that their architecture implies, also with respect to the nature of the data they are ready and accountable to manage so that users can make an informed choice.

3.7 Transfers of personal data

40 PIMS which follow the principles of data protection by design may help ensure that any transfer of personal data beyond the borders of the European Union will be done in compliance with the rules of the GDPR relating to international transfers.

41 PIMS may also help empower users to decide for themselves how far they wish to share their data geographically. Depending on the specifications of the individuals concerned, as gatekeepers, PIMS may help ensure that data will travel only insofar as the individual wishes it to do so.

42 Some individuals, for example, might not wish their health data to be transferred outside the European Union (or perhaps even to be shared beyond the borders of their own Member State). Some might opt for allowing transfers only to countries deemed to provide an adequate level of protection. Others may be more willing to take the risks of a broader data sharing. In this case, PIMS can also avail themselves of additional opportunities under the GDPR for the transfer of personal data. For example, they may enter into data transfer agreements with the recipients, which ensure that these recipients take upon themselves binding contractual obligations in compliance with the law.

3.8 Controllership and liability

43 PIMS can be considered intermediaries, or 'platforms' of a sort connecting two sides of the market: individuals offering their data for (re)use on the one hand, and organisations wishing to (re)use this data. Given this special situation, it is important for any PIMS to

clearly specify their role and liability vis-a-vis the individuals who entrust their data to them.

44 With respect to certain aspects of data processing, such as storage of data, there is usually no doubt that the PIMS will act as a controller, and therefore it is responsible for keeping the data secure. On this basis the PIMS will need to comply with all the provisions of the GDPR, for example those regulating security breaches.

45 In other cases, the analysis may be more complex, and it will be essential to clarify roles, responsibilities and liability[26]. For example, in case of a data breach or misuse of information by the customers of the PIMS (rather than the PIMS itself), to what extent: will the PIMS be liable? Will PIMS have any responsibility for screening and ensuring their customers are reliable?

46 Further, it should be made equally clear whether the PIMS themselves are entitled to further process the data, and if so, for what purposes and subject to what other terms and conditions.

47 In all aspects, whether with regard to its own data processing activities or those of its customers, it is also important to clarify whether, and to what extent PIMS may contractually limit their liability vis-a-vis the individuals' whose data they hold (it is to be noted, however, that in any event, as regards the liability of a PIMS as a controller, co-controller or a processor, Article 82 of the GDPR will apply, in any event).

3.9 Looking for a sustainable business model in the interest of the individuals

48 The current revenue model on the internet is primarily based on 'free' services provided to individuals in exchange of their personal data, making it a challenge to persuade a sufficient number of individuals to pay for PIMS. At the same time, organisations that hold large amounts of data may have a vested interest in keeping that data for themselves and under their control (as a competitive advantage) rather than enabling user control, whether through PIMS or other means (here the new right to data portability under the GDPR may provide some counterbalance).

49 PIMS can have clear advantages for online service providers. On the one hand, PIMS may facilitate compliance with the GDPR. On the other hand, they may provide a more complete, targeted and clean set of personal data from consumers. This would reduce the cost of accessing such data.

50 Possible business models for PIMS that could be viable for the individuals and the PIMS themselves include so-called "freemium" models vis-à-vis individuals: free basic functionalities, with additional functionalities, e.g. individual analytics on top of data against payment. Offering analytics-as-a-service on top of the data and fund the platform partly on this basis could represent in itself a privacy-preserving design facilitating big data analytics on top of personal information.

PIMS can also be offered as a service to companies or other organisations willing to improve their service offer to their clients through a privacy-friendly means of interaction. Revenue in this context would be generated by fees paid by the organisations using the data managed by the PIMS. Public sector bodies can likewise be clients when exploring personal information management in order to allow citizens to better manage access and use of their

data in an 'eGovernment' context, e.g. in a setting where the 'once-only' principle[27] is applied.

51 Another consideration is that some of the effects of using personal information (unsolicited advertisement and similar, price discrimination in the context of sales over the internet, other forms of discrimination or refusal of service and similar) may be regarded as negative externalities. If so, then it is perhaps unfair to ask the user to pay for enhanced privacy. Privacy is a fundamental right and should not become a privilege which can only be afforded by the richer parts of the population.

52 In any event, it is crucial to ensure the transparency of the business model vis-à-vis the individuals whose data are being processed so that they are aware of the interests at stake (of PIMS and other service providers) and can use PIMS in full awareness.

3.10 'Authorising use of' rather than 'selling' personal data

53 The model of PIMS seems to invite a debate over who 'owns' our personal data. Individuals in the EU have a fundamental right to the protection of their personal data, based upon Article 8 of the EU Charter of Fundamental Rights. Detailed rights and obligations relating to the exercise of this right are regulated in further detail in the recently adopted GDPR. These issues are not specific to PIMS: personal data is often perceived as the 'currency' we pay for so-called 'free' services on the internet. This trend does not, however, mean that personal data of individuals can legally be considered as property which can be traded freely as any other property on the market. On the contrary, as a matter of principle PIMS will not be in a position to 'sell' personal data, but rather, their role will be to allow third parties to use personal data, for specific purposes, and specifics periods of time, subject to terms and conditions identified by the individuals themselves, and all other safeguards provided by applicable data protection law.

4. CONCLUSIONS AND NEXT STEPS

4.1. Towards full application of the GDPR - opportunities

54 As noted above, the EU legislator recently adopted a data protection reform package that strengthens and modernises the regulatory framework so that it remains effective in the era of big data.

55 The new GDPR, including rules on increased transparency, and powerful rights of access and data portability, should help give individuals more control over their data, and may also contribute to more efficient markets for personal data, to the benefit of consumers and businesses alike.

56 Codes of conduct and certification schemes as provided for by the GDPR are privileged instruments to give specific visibility and role to technology and products that - like PIMS - may serve to more effectively implement data protection law at the practical level.

57 However, PIMS face the overarching difficulty of penetrating a market dominated by online services based on business models and technical architectures where individuals are not in control of their data, as explained in Section 3.9. Shifting to a situation where individuals have the effective possibility to give a service provider access to some data in their PIMS instead of providing the data directly to the service provider will require

additional incentives for the service providers. The Commission may use the initiatives it has announced on data flows and data ownership[28] to explore which additional policy initiatives could motivate data controllers to accept this way of providing data. Furthermore, an initiative by public eGovernment services to accept PIMS as a data source instead of direct data collection could add critical mass to the acceptance of PIMS.

58 This analysis could be complemented by measures aiming at laying the technical, societal and economic foundations, including standardisation efforts, economic incentives and fostering research and pilot projects.

59 The European Union and Member States public administrations, and projects co-financed by them, are the first places where this change of perspective should be tested, fostered and hopefully realised.

4.2. Supporting PIMS and underlying technology towards effective data protection

60 Good regulation, while crucial, is not sufficient in itself. As we stated in our Opinion on 'Meeting the challenges of big data'[29], companies and other organisations that invest a lot of effort into finding innovative ways to make use of personal data, should use the same innovative mind-set when implementing data protection principles.

61 The contribution of technology in the PIMS model is fundamental. PIMS can serve to test data protection by design approaches and technologies supporting them. Relevant research topics, where adequate support and investments are needed, include: interoperable and privacy-friendly identity management; authorisation mechanisms; data interoperability; data security; and mechanisms for automatic enforcement of established 'contracts' between individuals and other parties. All this is leveraged by cryptography and encryption and boosted by the cheap availability of computing power. Decisive support by policy makers, such as the Commission, to basic and applied research in these technology domains is necessary in this initial phase so as not to lose current opportunities.

62 In order to foster research and development and deployment to market in the area of PIMS, we recommend that the Commission plan for possible synergies with other areas of the Digital Single Market strategy, such as Cloud Computing and the Internet of Things. In this way, pilot projects could be carried out to design and test the interaction of cloud services and IoT with PIMS.

4.3. How the EDPS will advance this debate

63 The EDPS aims to contribute to fostering private and public efforts in the direction outlined above. We will continue to facilitate discussions, including via organisation of events/workshops, for example, with the view to identify, encourage and promote best practice to increase transparency and user control and explore the opportunities offered by PIMS. We will also continue to facilitate the work of the Internet Privacy Engineering Network (IPEN) as an interdisciplinary knowledge hub for engineers and privacy experts. In this context, we will continue to provide a platform for developers and promoters of PIMS to benefit from exchanges with specialists in other technologies and data protection.

Marrakesh, 20 October 2016

(**signed**)

Giovanni Buttarelli
European Data Protection Supervisor

Notes

[1] Communication COM(2014)442 on a thriving data-driven economy: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy.
[2] EDPS Opinion 7/2015: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf . See more specifically Section 3.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Official Journal of the European Union, L 119, Vol. 59, 4 May 2016, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.
[4] See inter alia Articles 6(1)(a), 7 and 8 and recitals 42-43 GDPR.
[5] Article 25 GDPR.
[6] Article 20 GDPR.
[7] Related concepts include 'personal data stores', 'personal data spaces' or 'personal data vaults.' We will use the term 'PIMS' in this Opinion, as it appears to best describe the concept in a general and easily understandable way. As used in this Opinion, the abbreviation 'PIMS' may refer to either the singular or the plural form: personal information management system or personal information management systems.
[8] See recital 7 GDPR: 'Natural persons should have control of their own personal data'. See also, for example, Doc Searls, *The Intention Economy: When Customers Take Charge* (Boston: Harvard Business Review Press, 2012).
[9] See, e.g. Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 2013, Vol 3, No 2.
[10] See, for example, the report on Personal Data Stores drafted by the University of Cambridge for the European Commission: https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school.
[11] See inter alia: Kai Rannenberg, Jan Camenisch, Ahmad Sabouri (eds.), *Attribute-based credentials for trust*, (Cham: Springer International Publishing, 2015).
[12] For more detail on the concept of anonymisation and its effectiveness see also Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[13] See for example the openPDS project: http://openpds.media.mit.edu/.
[14] For example see the Qiy Foundation (https://www.qiyfoundation.org/) and the Respect Network (https://www.respectnetwork.com/ and http://oixnet.org/registry/respect-network/).
[15] See EDPS preliminary Opinion on 'Privacy and competitiveness in the age of big data': https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf. In particular, see Section 4.2.2: *'Powerful or dominant undertakings are able to exploit "economies of aggregation" and create barriers to entry through their control of huge personal datasets alongside proprietary software which organises the data'.*
[16] A well-known effort was the P3P W3C project and the relevant preferences exchange language, APPEL.
[17] See, for example, the Kantara initiative (https://kantarainitiative.org/) under which umbrella many projects are carried out fostering 'privacy-respecting, secure access to trusted online services'.
[18] Article 4(11) GDPR.
[19] See Article 20 of the GDPR.
[20] Article 5(1)(d) GDPR.
[21] Article 5(1)(e) GDPR.
[22] A noticeable example is the use of the XDI protocol suite proposed by the XDI Public Trust Organisation (http://xdi.org/), allowing trusted and secure data exchange based on defined criteria (e.g. privacy preferences).
[23] Examples of these solutions are 'smart contracts' aiming at providing automated contract enforcement and negotiation. The concept dates back to when it was defined in the 1990's by cryptographer Nick Szabo (http://szabo.best.vwh.net/smart_contracts_idea.html). This concept has recently gained research momentum due to developments in cryptography.
[24] This usually happens also thanks to the involvement of identity/authentication providers, mutually trusted by all parties involved, which guarantee the authenticity of the data 'attributes' (privacy preferences or other pieces of information) and of the purposes/data uses advertised by online services as well as the identity of those

services. Furthermore, action can be performed upon certain events like successful or unsuccessful decryption such as notifications of the event to the PIMS, which enables control.

[25] Article 6(1)(c) and (e) GDPR.

[26] See also Article 82 GDPR.

[27] This refers to the principle that citizens should be requested by government to submit any given information or document only once in a setting where governmental authorities are then requested to share the information or document. It may appear desirable to foresee the storage of such information in a PIMS platform, to increase transparency and enable individuals to have better control over their data.

[28] Communication: Digitising European Industry - Reaping the full benefits of a Digital Single Market http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm.

[29] EDPS Opinion 7/2015, cited above.