

Executive Summary of the Opinion of the European Data Protection Supervisor on Personal Information Management Systems

(The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2016/C 463/10)

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 is 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.

I. 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⁾.

⁽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) (OJ L 119, 4.5.2016, p. 1).

⁽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.

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⁽¹⁾. 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.

IV. 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⁽²⁾ 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'⁽³⁾, 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.

⁽¹⁾ 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>

⁽²⁾ Communication: Digitising European Industry — Reaping the full benefits of a Digital Single Market http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm

⁽³⁾ EDPS Opinion 7/2015, cited above.

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.

Done at Marrakesh, 20 October 2016.

Giovanni BUTTARELLI

European Data Protection Supervisor
