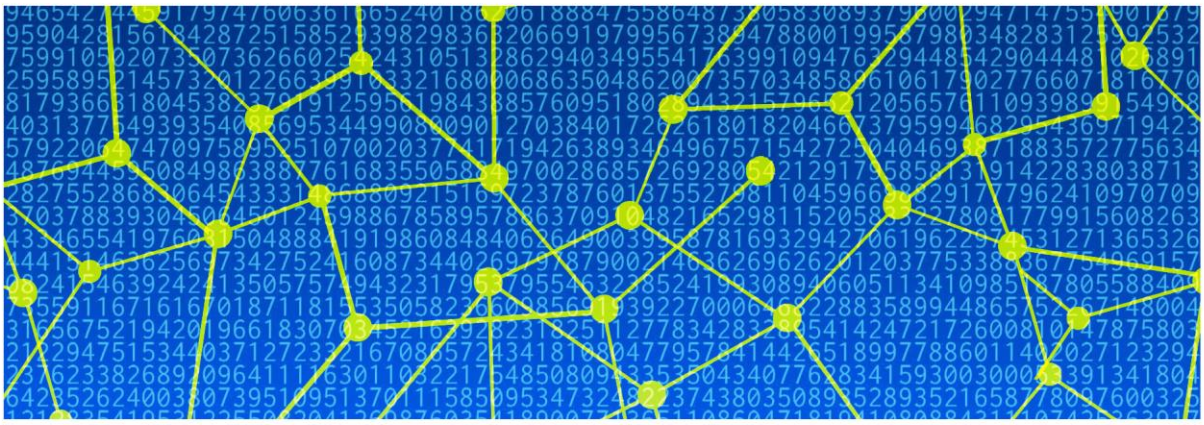

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2018

Preliminary Opinion on privacy by design

EDPS

31 May 2018

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 aims at contributing to the successful impact of the new obligation of "data protection by design and by default" as set forth by Article 25 of the General Data Protection Regulation by raising awareness, promoting relevant debate and proposing possible lines for action.

The principles of privacy by design and by default are explored in their historical development and in their translation into privacy engineering methodologies and privacy enhancing technologies.

This analysis is in context with the growing and widespread need for grounding technological development on human values and ethics. An effective implementation of the principle of privacy by design and by default can represent an outstanding milestone towards a human values based technology design.

Executive Summary

The possibilities and limits of technology play an increasingly important role in our personal lives and in our societies. The extent to which humans can enjoy their fundamental rights depends not only on legal frameworks and social norms, but also on the features of the technology at their disposal. Recent discoveries of inappropriate use of personal data have driven the public debate on data protection to an unprecedented level. It is necessary that the shaping and the use of technology takes account of the need to respect the rights of individuals, rather than being driven exclusively by economic interests of few businesses.

With the full applicability of the General Data Protection Regulation in the EU as of 25 May 2018, data protection by design and by default becomes an enforceable legal obligation. We need to keep the momentum going so that this new obligation can increase the effectiveness of the protection promised by the GDPR. This shall contribute to this target by raising awareness, promoting the creation of public value and societal wellbeing and by calling on all stakeholders to engage in a responsible discussion with a view to take the appropriate actions.

This Opinion distinguishes between the general principle of "Privacy by Design" which encompasses an ethical dimension consistent with the principles and values of the EU Charter of Fundamental Rights, and the specific legal obligations provided by Article 25 of the GDPR to which we refer as "Data Protection by Design" and "Data Protection by Default".

The Opinion briefly recalls the history of the principle of privacy by design from the initial research on technologies for privacy until the GDPR. It also analyses the content of Article 25 and its relationship with other articles. It also considers other elements of EU legislation which refer to privacy by design. Furthermore, some implementations outside the EU are presented.

In an overview of the state of the art, the Opinion provides examples of methodologies to identify privacy and data protection requirements and integrate them into privacy engineering processes with a view to implementing appropriate technological and organisational safeguards. Some of these methodologies define data protection goals directly from privacy and data protection principles, such as those of the GDPR, or derive them from operational intermediate goals. Other methodologies are driven by risk management. The design and operation process needs to consider the whole life cycle of a service or a product, from initial planning to service/product disposal. The technological overview includes also standardisation efforts to integrate privacy requirements in system design and the state of the art of privacy enhancing technologies.

There is a need to advance the state of the art and the use of privacy enhancing solutions. While research has been increasing as well as initiatives dedicated to the development of the privacy engineering discipline, this is not yet enough to drive a change in the effectiveness of the protection of individuals and their personal data. Organisations can only have benefits from adopting a privacy by design approach. Policies promoting privacy enhancing technologies and strategies should be within the priorities of the EU agenda and public administrations must lead by example. The IPEN initiative will be a vehicle to promote privacy enhancing technologies among stakeholders at the international level.

Initiatives for privacy by design should be seen in the broader context of integrating ethical considerations in technological design, following the conclusions of the recent report of the EDPS Ethics Advisory Group.

With this Opinion, the EDPS makes a number of recommendations to EU institutions:

- to ensure strong privacy protection, including privacy by design, in the ePrivacy Regulation.
- to support privacy in all legal frameworks which influence the design of technology, increasing incentives and substantiating obligations, including appropriate liability rules,
- to foster the roll-out and adoption of privacy by design approaches and PETs in the EU and at the Member States' level through appropriate implementing measures and policy initiatives,
- to ensure competence and resources for research and analysis on privacy engineering and privacy enhancing technologies at EU level, by ENISA or other entities,
- to support the development of new practices and business models through the research and technology development instruments of the EU,
- to support EU and national public administrations to integrate appropriate privacy by design requirements in public procurement,
- to support an inventory and observatory of the "state of the art" of privacy engineering and PETs and their advancement.

The EDPS will:

- continue to promote privacy by design, where appropriate in cooperation with other data protection authorities in the European Data Protection Board (EDPB),
- support coordinated and effective enforcement of Article 25 of the GDPR and related provisions,
- provide guidance to controllers on the appropriate implementation of the principle laid down in the legal base, and
- together with the DPAs of Austria, Ireland and Schleswig-Holstein, award privacy friendly apps in the mobile health domain.

Coordination and joint efforts of the technological capabilities among the Data Protection Authorities are essential to promote data protection by design and by default. Cooperation in the EDPB, as well as the International Working Group on Data Protection and Telecommunications (IWGDPT, "Berlin Group") is necessary.

We welcome feedback to this preliminary Opinion.

The 2018 International Conference of Privacy and Data Protection will be a milestone in the discussions about a digital ethics in general and an opportunity to better define the way forward for privacy by design.

TABLE OF CONTENTS

1. Privacy by design and by default: an opportunity for effective protection of individuals

1.1 Why an Opinion on "Privacy by Design"

1. In early 2018, the public debate about the processing of personal data with advanced information and communications technology has reached an unprecedented level of attention. Parliamentary committees are performing or considering investigations at the European Parliament[1], the US Congress[2], and national parliaments of EU Member States such as the UK[3], Germany[4] and France[5]. Members of these Parliaments, as the general public[6], want to understand how their personal data are processed and used in the tracking of citizens' activities on the web and the processing of the collected personal data. For these investigations, hearings of executives from technology companies play a central role.

2. Despite the huge media interest, the public is still only aware of "the tip of the iceberg"[7] with respect to tracking and targeting. The EDPS has analysed the use of personal data for online manipulation in its recent Opinion[8] and has provided recommendations on enforcement of data protection law, common analysis and cooperation of regulators across sectors, self-regulation and empowerment of individuals. The Opinion also notes that the recent discoveries underline the importance of designing technologies so that they support the practical and effective exercise of fundamental rights, rather than being driven exclusively by economic interests of businesses.

3. The present Opinion builds on many years of work of privacy and technology experts on the role of technological design for ensuring the fundamental right of privacy. It takes stock of legal and technological developments across the globe and provides recommendations for measures that shall further advance privacy and data protection by design. While the observations on online manipulation make the urgency of a new approach in technology design very visible, and while the systems used on the Internet play a central role, the need to ensure that fundamental rights are taken into account for technological development applies to all data processing tools, regardless of the platforms and application areas used.

"Privacy by Design" or "Data Protection by Design"?

4. For the purpose of this Opinion, we use the term "privacy by design" to designate the broad concept of technological measures for ensuring privacy as it has developed in the international debate over the last few decades. In contrast, we use the terms "data protection by design" and "data protection by default" to designate the specific legal obligations established by Article 25 of the GDPR [9]. While measures taken under these obligations will also contribute to achieving the more general objective of "privacy by design", we consider that a wider spectrum of approaches may be taken into account for the objective of "privacy by design" which includes a visionary and ethical dimension, consistent with the principles and values enshrined in the EU Charter of Fundamental Rights of the EU.

Does technology shape society, or does society shape technology?

5. Technology is linked to the evolution of mankind since the first man-made tools. Technological progress has heavily impacted the evolution of human societies, often for the

best, sometimes for the worst. The rules that govern our societies, both as binding laws and as social norms, are also heavily influenced by technology. Data protection is a good example of this interaction as the birth of this legal concept is linked to the development and popularisation of the computers first, and, more recently, of the Internet. The programmatic words of recital 2 of the Data Protection Directive[10] ("*whereas data-processing systems are designed to serve man*") and recital 4 of the GDPR ("*the processing of personal data should be designed to serve mankind*") fully illustrate this point. The example of data protection shows the complexity of the interaction between technology and rules: while the concept of data protection itself was developed in reaction to the emerging power of computing in administration and business, it took several decades until the obligation to integrate data protection safeguards in the technological design became an explicit legal obligation.

6. In 1989, two developments marked the beginning of a transformation which eventually turned the Internet into the dominant communications infrastructure of today. While, for its first 20 years, the Internet had been used mainly by research and scientific institutions, civilian and military, it was opened for public commercial use by connecting it to existing e-mail services. In the same year, Sir Tim Berners-Lee's proposal for a distributed hypertext system using links and universal resource locators laid the foundation for the World Wide Web with its seemingly unlimited potential to organise information and make it accessible at global scale.

7. Both the Internet and the World Wide Web have been continuously developed and modified over the last 29 years, and are still growing in size, capacity and capabilities. Cookies, scripting languages, compressed audio-visual formats, search engines, streaming protocols, social media platforms, smart mobile devices, tracking, analytics and profiling tools have enabled new ways of use and of conducting business. While many benefits are obvious, serious concerns about their impact on fundamental rights and the very foundations and the functioning of democratic societies are on the raise. Loss of control over personal data, the distribution of fake news and targeted political advertising, based on analysis and evaluation of personal data, are some of the challenges recently identified[11]. In his 2018 address on the occasion of the WWW anniversary, Sir Tim Berners-Lee observes that more than half of the world's population will have access to the Web, but that the Web now is under control of very few powerful platform companies, who have the power to decide which ideas and innovations are being pursued, excluding most of the world's population from having a say on its development, and at the same time making advertising the Web's dominant driver[12].

8. While our parliaments and our societies are still figuring out how to deal with these challenges, new technological developments are likely to cause even greater and deeper changes to human communication and social interaction. The processing of huge amounts of information, Big Data, is constantly increasing. The Internet of Things is still in the early stages of its deployment and the number of connected devices is expected to grow by an order of magnitude at least, becoming more pervasive not only in homes and cities, but in the human body itself[13]. The development of Artificial Intelligence is only just beginning to move from narrow specialised fields into broad application. Blockchain technology is promoted for wide uses, including for the processing of personal data. Business and engineering decisions about the future development of these technologies that are being taken now are likely to have long-lasting effects for us and our descendants.

9. We have observed a successful effort to shape technology according to societal objectives with the sustainability principles developed over the last decades for the preservation of the

natural resources[14]. As in environment law, technology must be designed and implemented for its entire lifecycle in a way compatible with the fundamental rights and values that determine our democratic societies. This experience inspires confidence that it is possible to take control of technology for the best of humans. Research in the history of technology has shown that "*Technology is neither good nor bad, nor is it neutral*"[15], that its development is not subject to inherent determinism and that it can be shaped: "*Although technology might be a prime element in many public issues, nontechnical factors take precedence in technology-policy decisions*"[16]. The EDPS has fostered an analysis of broader ethical demands over the last couple of years in the context of the works of the Ethics Advisory Group[17] set up in 2015.

10. The EU has adopted specific provisions on the shaping of technological solutions when there is processing of personal data. Since 25 May 2018, when the GDPR[18] became fully applicable, data protection by design and by default are no longer only a desideratum or recommended good practice, but a legal and fully enforceable obligation that all those who process personal data under EU law must comply with. We need to keep the momentum going so that this new obligation can materialise and increase the effectiveness of the protection promised by the GDPR, and not construed too narrowly.

11. This EDPS Opinion aims at contributing to this process by raising awareness and promoting the creation of public value and societal wellbeing and calls on the relevant stakeholders (EU and national policy makers, data protection and other regulators, academia, technology providers, private and public organisations responsible for processing personal data and individuals whose data are being processed) to engage in a responsible discussion in order to take the right decisions bearing in mind not only the progress of technology and its endless capabilities but also the fundamental rights at stake, among which there are privacy and the protection of personal data.

12. While Article 25 of the GDPR represents an important milestone in the endeavour towards responsible technology design and operation, and while the way this new legal principle is implemented and enforced will be a key success factor for the whole new legal data protection framework, this Opinion does not include a comprehensive legal analysis of Article 25 of the GDPR[19], nor does it contain step by step guidance[20] for organisations to comply with Article 25. It rather aims at identifying essential elements that can ease the understanding of the main principle and its consequences for all stakeholders concerned, conveying clear messages in plain language to foster a fruitful debate. Detailed guidance on Article 25 can be expected to be provided by supervisory authorities and the EDPB.

1.2 History of Privacy by Design

13. In the past, privacy and data protection have been perceived by many organisations as an issue mainly related to legal compliance, often confined to the mere formal process of issuing long privacy policies covering any potential eventuality and reacting to incidents in order to minimise the damage to their own interests. In other words, for many organisations, data protection has been limited to "window dressing" with very little impact on the organisational objectives or practices or for the protection of the individuals concerned.

14. The **difficulty of translating legal principles into actionable requirements** and the need for a truly multidisciplinary approach[21] to tackle privacy issues have contributed to widen the gap between a legal compliance discipline managed by lawyers, on the one hand, and a dynamic innovation process driven by business managers and engineers on the other hand,

who are ultimately responsible for the design and implementation of the processes and systems that govern the real functioning of the organisation.

15. Against this background, the idea that technology development is not only the cause of increasing privacy concerns but also part of the solution was born not later than the codification of privacy principles into best practices and law, i.e. as of the 1970's. David Chaum and others[22] conducted initial technology research clearly oriented to address privacy concerns with contributions on data minimisations, anonymous transactions and communications, as well as technologies for privacy in statistical records. Enhancements in communication technology, IT security (including conceptual frameworks designed to empower the end user of ICT system with more self-determination in privacy and security[23]), in anonymous communications and in cryptography paved the way to the development of what became to be known as Privacy Enhancing Technologies (PETs)[24], a family of technological solutions oriented to minimise the privacy risks to individuals.

16. Yet neither security nor privacy were really integrated as primary requirements in the development and expansion of Internet and WWW, and priority was given to functionality, scalability and openness. After revelations on programs of mass surveillance by national security agencies in 2013[25] the Internet Engineering Task Force (IETF)[26] made a statement[27] acknowledging that "*the scale of recently reported monitoring is surprising. Such scale was not envisaged during the design of many Internet protocols...*" Works towards more integration of privacy in internet protocols were then kick-started with the IETF Vancouver meeting in November 2013.

17. The term "privacy by design" was originally used by Ann Cavoukian when she was the Information and Privacy Commissioner of Ontario, Canada. In her concept, privacy by design can be broken down into "7 foundational principles"[28], emphasising the need to be proactive in considering the privacy requirements as of the design phase throughout the entire data lifecycle, to be "*embedded into the design and architecture of IT systems and business practices...without diminishing functionality...*", with privacy as the default settings, end-to-end security including secure data destruction and strong transparency subject to independent verification. The principle of privacy by default was elicited as the second of the foundational principles, establishing that privacy by design involves *"ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default*". This statement, is a powerful operational definition of the principle of privacy by default, where the individual does not bear the burden of striving for protection when using a service or a product but enjoys "automatically" (no need for active behaviour) the fundamental right of privacy and personal data protection.

18. Some elements of the principle of privacy by design can already be found in the Data Protection Directive 95/46/EC[29] (hereinafter "the Directive"), repealed by the GDPR. Recital 46 of the Directive highlights how the technical and organisational measures to be taken to protect rights and freedoms of people whose data are processed should be applied "*both at the time of the design of the processing system and at the time of the processing itself ...*".

19. The "Resolution on Privacy by Design" adopted by the 32th Conference of Data Protection and Privacy Commissioners in October 2010[30] represents a landmark in the recognition of

the principle as "*essential component of fundamental privacy protection*". The Conference invited data protection authorities to foster privacy by design in the "*formulation of policies and legislation within their respective jurisdictions*".

20. The Article 29 Working Party (WP29)[31] in its reply to the European Commission public consultation for the data protection reform demanded the introduction of the principle of privacy by design into the new legislative framework because "*Whereas the above provisions of the Directive are helpful towards the promotion of privacy by design, in practice they have not been sufficient in ensuring that privacy is embedded in ICT*", asking also for "*privacy by default settings*". The WP29 went on by recommending that this "*principle should be binding for technology designers and producers as well as for data controllers...They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems".*

21. In its "Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy" of March 2010[32], the EDPS fully endorsed the principle of privacy by design as the key tool for increasing trust in information technology and made a comprehensive analysis with specific recommendations. We indicated how the principle should have been embedded in general and sectorial personal data protection legislation (including social networks, the internet of things, RFID devices and browsers). We also made recommendations on how to foster the implementation of the principle in IT products and services, once acknowledged that PETs had not substantially made it to the market and analysed the possible reasons, including lack of economic incentives, institutional support and insufficient user demand.

22. While privacy by design has made significant progress in legal, technological and conceptual development, it is still far from unfolding its full potential for the protection of the fundamental rights of individuals. The following sections of this Opinion provide an overview of relevant developments and recommend further efforts.

2. Data protection by design and by default in EU law

2.1. Article 25 of the GDPR

23. Article 25[33] of the GDPR, titled "Data protection by design and by default" [34], provides that the controller[35] shall implement appropriate technical and organisational measures, both at the design phase of the processing and at its operation, to effectively integrate the data protection safeguards to comply with the Regulation and protect the fundamental rights of the individuals whose data are processed. Those measures shall be identified taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing as well as the risks for the rights and freedoms of those individuals. The Article states that, by default, only personal data that are necessary for each specific purpose of the processing may be processed. The Article concludes that approved certification mechanisms may be used to demonstrate compliance with the set requirements[36].

24. The data protection by design and by default requirement of Article 25 complements the controller's responsibility laid down in Article 24, a core provision of the GDPR. This article defines "who shall do what" to protect individuals and their personal data and states that a risk-based approach shall be adopted to identify what needs to be done to that purpose. More precisely, it provides for the controller to *"implement appropriate technical and*

organisational measures to ensure and to be able to demonstrate that processing is performed in accordance..." with the law. These measures shall be designed *"taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons*".

25. These include the rules of Article 32, which requires an IT security risk management framework and measures to mitigate risks for the individuals whose data are processed by adequately securing those data. It is useful to remind that, whereas the measures identified in Article 32 are just those targeting one of the data protection principles in Article 5[37], namely the one called "integrity and confidentiality", Article 24 refers to the implementation of all data protection principles and the compliance with the whole of the GDPR.

26. In the context of the controller's responsibility to ensure and to be able to demonstrate compliance with the law, Article 25 aims at technical and organisational measures as required by Article 24, stressing some dimensions of their implementation process already implicitly present in Article 24 and adding others, making them all mandatory. We describe these dimensions in the following paragraphs.

The various dimensions of the obligation of data protection by design

27. The first dimension is acknowledging the fact that processing of personal data, partially or completely supported by IT systems should always be the **outcome of a design project**. Article 25 requires consideration of safeguards[38] both at the design and operational phase, thus **aiming at the whole project lifecycle**[39] and clearly identifying the **protection of individuals and their personal data within the project requirements**.

28. The second dimension is the **risk management approach** with a view to selecting and implementing **measures** for effective protection. The **assets to protect are the individuals** whose data are processed and in particular their fundamental rights and freedoms[40]. In this respect, there is no indication of obligatory measures[41]. Nonetheless, the legislator gives directions on those factors (nature, scope, context and purposes of processing) that the organisation must take into account in the selection of the appropriate measures.

29. At the same time, the organisation is responsible for choosing the safeguards among those available (within the "state of the art") and consider their cost among the elements leading to the final decision, weighed against the risks for individuals. These two factors, the state of the art of available technology and the cost of implementation of the measures, must not be interpreted in such a way that the measures chosen do not sufficiently mitigate existing risks and the resulting protection is not adequate.

30. The third dimension is the need for these **measures to be appropriate and effective**. The effectiveness is to be benchmarked against the purpose of those measures: to ensure and be able to demonstrate compliance with the GDPR, to implement the data protection principles and to protect the rights of individuals whose data are processed. In particular, Article 25 provides for those measures to be designed "*to implement data protection principles ... in an effective manner*". These data protection principles, set out in Article 5, can be considered as the **goals to achieve**. They have been singled out by the legislator as a cornerstone for the protection of individuals when processing their data and are complemented in the GDPR by either more detailed rules (i.e. the information to provide to the individuals and their rights as "data subjects"[42], which are further elaborated on the "transparency" principle; or

the security obligations of Article 32) or by other accountability instruments, such as the documentation duties of Article 30, which are instrumental to those principles. This means that effectively meeting those principles/goals, as further detailed in the law by other provisions, would ensure the expected protection of personal data.

31. The fourth dimension is the obligation to **integrate the identified safeguards into the processing**. The GDPR includes some safeguards to protect the individuals whose data are processed through means that are "external" to the processing itself, such as data protection notices for example. This dimension instead focuses on the need to protect the individuals by directly protecting their data and the way they are managed.

32. All four dimensions are equally important and become an integral part of accountability and will be subject to supervision from the competent data protection supervisory authorities where appropriate.

The obligation of data protection by default

33. Following the application of the principle of data protection by design, organisations must, by default, only process personal data necessary for each specific purpose defined in compliance with the law and transparently notified to the individuals concerned. While it can be argued that this obligation is already implicit in the "purpose limitation" and "data minimisation" principles[43] in both the design and operation phases[44], the explicit rule stresses the importance of taking technical measures to meet the expectations of the individuals whose data are processed, not to have their data processed for other purposes than what the product and service is basically and strictly meant to do, leaving by default any further use turned off, for instance through configuration settings[45].

34. Some of the added value of the data protection by default provision is also the further elaboration of the principle of data minimisation and the extension to the principle of storage limitation. Article 25(2) explains how the obligation to process by default only personal data that are necessary "*applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility...*". The Article then establishes a precise obligation by instantiating the general principle in one particular use case: organisations shall set up measures to prevent personal data from being made public by default.

The role of "processors" and relevant duties of controllers

35. Providers of services to an organisation that process personal data on the organisation's behalf are considered as "processors"[46] in the GDPR. It is a duty for the organisation/controller to choose contractors/processors that are able to support them in complying with the law[47], and thus also with the data protection by design and by default obligations.

36. This indirectly obliges those processors to design and operate processes and technology so as to enable the responsible organisation to protect the individuals and their data in a data protection by design and by default approach.

Article 25 and developers of products and technology

37. A serious limitation of the obligations of Article 25 is that they apply only to impose an obligation on controllers and not to the developers of those products and technology used to

process personal data. The obligation for products and technology providers is not included in the substantial provisions of the GDPR. However, Recital[48] 78 states that *"When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*...". Thus, the application of Article 25 would require the provider to design their products in such a way as to enable the controller to put in place all the necessary measures needed to protect the individuals and their data, and configure them in a way that by default, without any user intervention, no personal data at all are collected or at least only those that are strictly necessary to carry out what can be expected from the basic utilisation of that product.

Article 25 and public administrations

38. Article 25 applies to all types of organisations acting as controllers, including public administrations, which, considering their role to serve the public good, should give the example in protecting individuals' fundamental rights and freedoms. The GDPR stresses the role of data protection by design and by default when public administrations need to identify their providers of products and services in Recital 78, stating the *"The principles of data protection by design and by default should also be taken into consideration in the context of public tenders*". Public administration are called be in the frontline in applying these principles in an accountable way, ready to demonstrate their implementation, if necessary, to the competent supervisory authority.

Data protection impact assessment

39. Article 35 of the GDPR provides for a mandatory Data Protection Impact Assessment (DPIA) when the processing is *"likely to result in a high risk to the rights and freedoms of natural persons*...". This obligation complements the **mandatory risk management approach** of Article 24 when the organisation estimates that the level of risk for the individuals whose data are processed is high[49]. The DPIA represents an outstanding accountability tool and organisations may benefit from adopting this approach also in cases where it is not mandatory[50].

40. In its guidelines on DPIA[51], the WP29 stated that it serves as a data protection by design safeguard because it "*should be carried out prior to the processing*...". This is consistent with the data protection by design and by default principles[52]. The management of data protection risks, is at the core of the privacy by design and by default approach.

2.2. Privacy by design and data protection by design in EU sectorial rules

41. In addition to the GDPR, there are several provisions in EU sectorial law related to the principles of privacy by design and by default.

The Directive on privacy and electronic communications and the Radio Equipment Directive

42. The principles of privacy by design and by default do not appear explicitly in the substantive provisions of the ePrivacy Directive[53]. Yet Recital 30 specifies that "*Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum*...". This is a recommendation

for providers of public electronic communication services **and products** to engineer those services in a way as to respect the data minimisation principle.

43. Recital 46 states that "*The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service...*" and thus recalls the need for overarching protection. Then it goes on by saying that "*It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected*" and explicitly refers to the measures to be adopted in accordance with the Directive 1999/5/EC[54] on radio equipment and telecommunications terminal equipment. Directive 2014/53/EU[55], repealing it, and replacing relevant rules for radio equipment's, explicitly provides in Article 3(3)(e) that certain radio equipment *"shall be constructed...*" in a way as to incorporate *"safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected*". We can note, also in this obligation, a reference to the **engineering phase of products.**

44. The EDPS Opinion[56] on the Commission proposal to replace the ePrivacy Directive[57] with the new ePrivacy Regulation is coherent with the approach of Recital 78 of the GDPR and proposes for the sector "*an obligation on hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices*". This obligation would be on **providers of hardware and software for all kind of communication services**, including instant messaging, voice over IP, and communications of personal data among "objects" in the Internet of Things and website operators. This provision would highly increase the standard of protection and enable all providers of electronic communication services with a real opportunity to be compliant and not dismiss any claim of low protection by pointing their fingers to the unavailability of appropriate suppliers. It would also represent a reference with a view to a possible extension of a similar provision in other sectors.

eIDAS Regulation

45. The eIDAS Regulation[58] provides the framework for the provision of electronic identity and trust services in the digital single market of the EU. As the provision of such services requires the processing of personal data by the service provider, the Regulation contains references to the Data Protection Directive. In addition to compliance with data protection principles, the Regulation also refers explicitly to privacy by design as a principle to be supported by the eIDAS interoperability framework. The technical implementation of eIDAS services should be guided by a common interoperability framework which implements the principle of privacy by design[59]. However, it would be necessary to adjust the measures implemented under the eIDAS Regulation in order to develop this potential.

Smart metering and smart grids for energy and gas: a case of co-regulation

46. For the energy sector, and more precisely the roll-out of smart metering systems in the EU, the data protection by design principle has been substantiated in a more comprehensive way. In 2012 the Commission issued a Recommendation[60] on the preparation for the roll out of smart metering systems in the electricity and the gas markets to provide guidance to Member States on data protection by design and by default and the application of data protection principles. The Recommendation established that Member States should adopt and apply a

template for a data protection impact assessment ('DPIA Template') and then ensure that network operators and operators of smart metering systems take the appropriate technical and organisational measures to ensure protection of personal data in accordance with the DPIA Template. The Template was prepared by the industry with the help and coordination of the Commission and submitted twice to the WP29 for an opinion. It was annexed to a Commission Recommendation adopted in October 2014[61].

47. Recital 17 of the DPIA Template Recommendation explains: "*Such a Template should facilitate the application of the principle of data protection by design by encouraging data controllers to carry out an impact assessment of data protection as soon as possible, hence allowing them to anticipate potential impacts on the rights and freedoms of data subjects and implement stringent safeguards. Such measures should be monitored and reviewed by the data controller throughout the lifecycle of the application or system*". This is in line with the **central role of the data protection risk management** process, as stated in paragraph 39, and with the need to consider **privacy requirements at early stages and along the whole lifecycle** of a project, as highlighted in paragraph 27.

48. Recommendation 2012/148/EU also triggered the initiative to identify Best Available Techniques[62] for the cybersecurity and privacy of smart metering system on the basis of 10 minimum functional requirements. The term 'Best Available Techniques'(BAT) [63] refers *"to the most effective and advanced stage in the development of activities and their methods of operation, which indicates the practical suitability of particular techniques for providing the basis for complying with the EU data protection framework. They are designed to prevent or mitigate risks to privacy, personal data and security*".

49. Within the meaning of the Article 25 of the GDPR, the catalogue of BATs corresponds to an indication of the state of the art for technical and organisational measures, where effectiveness of the measures, maturity of the technique and the cost of implementation are taken into account. Furthermore, BATs focussing on privacy may also be seen as PETs.

50. We believe that some elements of the work carried out in the smart metering sector, and in particular the approach of inventorying best available techniques for privacy, could contribute to operationalising privacy by design in different technological sectors.

3. The international dimension of privacy by design

51. The adoption of the privacy and data protection by design and by default principles is not just an EU concept: as a significant part of its development was driven on the other side of the Atlantic. The 7 foundational principles[64], as relayed by privacy commissioners in the Jerusalem Declaration[65], the research in privacy enhancing technologies and the efforts to engineer privacy requirements systems and processes, have influenced privacy guidance and the definition of best practices and emerging standards worldwide. Privacy by design has been proposed recently as a principle to be included in other national laws[66].

52. Examples of countries where the privacy by design and by default approach has widely been brought forward by competent authorities are Canada, Australia[67] and the US, often in parallel with the use of Privacy Impact Assessments (PIAs), identified as "the" methodological step qualifying the overall approach to be carried out in early stages of the project and used to elicit requirements via the assessment of data protection risks. The approach has benefited from the wider scope of the PIA often going beyond the strict

protection of personal data, encompassing the wider, multidisciplinary and contextual concept of privacy and even other fundamental rights as targets.

53. A 2012 report[68] by the US Federal Trade Commission (FTC) proposed privacy by design as one of the three main concepts[69] of a new framework that would "*incorporate the full set of fair information practice principles, updated for the 21st century*"[70]. Privacy by design *"must be something that an engineer or website developer instinctively thinks about when writing code or developing a new product. Respecting privacy must be considered integral to the innovation process...helps lift the burden of privacy protection off the shoulders of consumers...Too often, privacy protection depends on the notion that consumers can read and understand the legalese of lengthy privacy policies. The FTC's new framework seeks to steer away from that unrealistic vision of privacy protection"*[71].

54. The FTC framework is different from the GDPR in terms of scope of application[72], legal nature[73] and some substantial differences may be found in the legal interpretation of some of the privacy principles it aims at implementing (e.g. the lawfulness in data protection principles of Article 5 of the GDPR, including the strict necessity test of data processing). Nevertheless, the FTC definition of privacy by design can be seen as quite similar (methodologically and even substantially to a large extent) to what is in the EU law in all its dimensions as outlined in section 2.1, and is clearly formulated with a view to the practical implementation of the principle.

55. While the FTC framework and other related initiatives have contributed to the conceptual development of privacy by design and of technological means, there has not been an appropriate follow up by legislative developments and therefore they have not had the profound and far reaching impact that they could have had with the full commitment of the legislator.

56. More recently, the National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce, has issued an Internal Report featuring an introduction to the concepts of privacy engineering and risk management for US federal systems[74]. This represents an outstanding novelty in the panorama of guidance provided by governments or data protection authorities as the document includes a privacy risk model and a methodology to implement privacy requirements when engineering systems processing personal data. NIST documents are considered as standards for US federal information systems and should be met by federal agencies[75]. The NIST privacy engineering program continues[76].

4. Designing and operating procedures and systems while protecting personal data

4.1. Operationalising privacy and data protection by design and by default

57. EU data protection law and other privacy frameworks, such as the Fair Information Practice Principles[77] or the OECD guidelines[78] specify objectives to meet without usually giving guidance on how to meet them in practice. Applying the principle of privacy by design can help to solve this issue as it translates into practical guidance, to:

    1. define a methodology to integrate privacy and data protection requirements as part of projects aiming at developing and operating a process, procedure or system processing personal data;

2. identify and implement adequate technical and organisational measures to be integrated in those processes, procedures and systems to protect individuals and their data. Technological innovation can be a tool to support those measures;

3. integrate the support for privacy in the management and governance framework of the organisation, by identifying tasks and defining and allocating resources and responsibilities.

58. There have been methodologies in place to define the requirements for business processes and IT systems for a long time[79]. In particular, there is a common understanding of how requirements should be prepared for IT systems and many best practices have been proposed and adopted by academia and industry. Usually requirements have been broken down into functional and non-functional ones. Functional requirements are those that define the main business purpose and the specificity of the system to be developed. Non-functional requirements[80] apply to all systems and concern horizontal issues, such as security needs and compliance with applicable laws. Privacy and data protection should be considered within the non-functional requirements[81].

59. For many reasons, though, privacy has often been forgotten or considered as an afterthought when designing systems. Reasons for this include the contextual and often culturally dependent concept of privacy and the difficulty of translating privacy objectives into actionable requirements. The European Union Agency for Network and Information Security (ENISA) has issued a wide-ranging analysis of the state of the art of how to engineer privacy by design in December 2014[82].

4.2. Engineering privacy and data protection

Identifying data protection requirements and selecting adequate measures to meet the requirements

60. Some current privacy engineering methodologies work by defining data protection goals either directly from the data protection principles or defining operational intermediate goals that allow to meet the original ones. Other methodologies are more explicitly driven by a risk management approach, by identifying and tackling the risk of not meeting the data protection principles and/or by directly assessing possible adverse impact on individuals.

61. In section 2.1 we say that the GDPR looks at those principles as goals to achieve, used as "proxies" to protect individuals' fundamental rights and freedoms, independently from the level of risk. At the same time it adopts a "precautionary" approach and identifies safeguards to be implemented in all circumstances under certain conditions (e.g. security measures, personal data breach notifications etc.). What is left to effectively achieve the expected protection of individuals and grant them the established data protection rights, because of context, nature of data, type of processing etc., is then accounted for by the risk management approach. This approach enables organisations to identify new measures and contributes to detailing and integrating what is already mandatory based on the risk of the individuals.

62. Software development methodologies have inspired the approach to use a catalogue of specific design patterns to develop solutions to known privacy problems. This aspect is further developed in paragraph 72.

Examples of existing methodologies

63. Based on the definition of privacy and data protection objectives, it has become possible to develop design methodologies in which the corresponding requirements can be fully integrated. A brief introduction on some of these methodologies is provided in this section and the interested reader may consult the source documents for fuller appreciation.

64. The "Six protection goals for privacy engineering"[83] provide a framework to identify safeguards for IT systems processing personal data. Besides the classical IT security triad[84] of "confidentiality", "integrity" and "availability", three additional goals[85] follow: "unlinkability", "transparency" and "intervenability". IT security in this context does not target risks for the organisation but rather risks for the rights of individuals. Any usual approach known in IT security risk management literature can be used if it is clear what the assets to protect are (the individuals).

65. "Unlinkability" relates to the ability of pieces of information to be related to each other and to an individual. Anonymity clearly falls within it. "Transparency" implies that "*all privacy-relevant data processing including the legal, technical, and organizational setting-can be understood and reconstructed at any time... Furthermore, it is a prerequisite for accountability. Standard methods for achieving or supporting transparency comprise logging and reporting, documentation of the data processing, or user notifications"*. "Intervenability" enables "*the effective enforcement of changes and corrective measures*" and is relevant to enable individuals' rights and the possible intervention of competent authorities.

66. These goals are inter-related and help show, among others, that privacy measures could conflict with each other. For example, logging operations on personal data at the service of intervenability increases the risk of missing the "unlinkability" goal by creating the risk of a misuse of the logged operations. To complete the picture, these goals could be used with a methodology to elicit safeguards to meet them, as well as efforts exist to have a catalogue of possible measures serving those goals.

67. The US NIST[86] has adopted a definition of privacy engineering as a "*specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII[87]"*. NIST considers privacy engineering as made up of many components whose foundational elements are a risk management framework and engineering objectives. They identify a privacy risk model and three privacy system objectives on top of the classical security objectives represented always by the confidentiality, integrity and availability: predictability, manageability and disassociability. The three objectives help engineer systems to meet the privacy principles[88], as illustrated in the document of reference[89].

68. "Predictability" is about "*enabling reliable assumptions by individuals, owners and operators about PII and its processing by an information system*". This means integrating mechanisms ensuring and providing evidence to stakeholders that what should be done to protect individuals and their data is there and is effective. For example, engineering a mechanism to enable consent management and giving evidence of what has been selected would meet the predictability goal. "Manageability" means "*providing the capability for granular administration of PII including alteration, deletion, and selective disclosure*", which are essential for proper personal data management. "Disassociability" enables "*the processing of PII or events without association to individuals or devices beyond the*

operational requirements of the system". This privacy objective clearly focuses on minimisation of personal data and possible anonymisation.

69. In the NIST privacy engineering methodology, predictability stands out as a sort of meta-objective providing the basis for effectiveness in the implementation of measures, as well as transparency and accountability of the solutions proposed towards the stakeholders (individuals, competent authorities, society etc.). One practical example of how implementing this objective are measures such as the use of cryptography to give mathematical evidence of facts.

70. Another example of a privacy engineering methodology, in this particular case stressing the risk analysis dimension, is the LINDDUN[90] approach developed at Leuven University. It entails:

- creating data flow diagram based on the high-level system description;
- mapping the following privacy threat categories: linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance, as identified by the methodologies, onto the diagram elements;
- identifying those elements of the data flow diagrams where these threats could pose a risk and performing a risk analysis using the privacy threat tree patterns provided by the methodology. Threats are then prioritised based on the assessment. LINDDUN does not indicate how to perform the assessment of risks. This means that the criteria leading to the prioritisation of the risks are left to the organisation implementing the methodology, which gives some flexibility to the organisation;
- based on the prioritisation of risks, mitigation strategies and specific solutions are chosen as relevant for the specific threats. The methodology provides a taxonomy of mitigation strategies, which can be integrated and detailed as needed. PETs are then to be selected to effectively implement those strategies.

71. Risk management is at the core of the LINDDUN methodology, complemented by a catalogue of high level, technology neutral strategies, to be implemented by organisational measures and state of the art technological solutions.

72. Another approach of identifying measures to implement privacy requirements is the identification of "patterns" to engineer IT solutions to privacy requirements. "Design patterns", as defined in software development methodologies to solve recurrent problems[91], are proposed as building blocks to implement privacy measures in systems[92] in the context of a strategy (and a tactic). These patterns are then practically implemented in software building blocks and supported by PETs. "Design strategies" for commonly known privacy related problems are identified[93] describing "*a fundamental approach to achieve a certain design goal*". For better modelling they may be broken down into a further, more specific, abstraction layers (e.g. in so called "tactics", as "*approaches to privacy by design which contribute to an overarching strategy*").

Addressing the entire lifecycle of services and products, organisational governance and management

73. While some privacy engineering methodologies mainly focus on the requirements phase or the measures to implement, privacy engineering must consider the whole life cycle of a service or a product, from initial planning to service/product disposal. Adequate governance and management structures and procedures in the organisation are then needed to enable the overall approach.

74. An example for a methodology focused on the whole project lifecycle is the one issued by the PRIPARE research project[94]. It proposes comprehensive privacy related actions and deliverables along eight project phases, from the considerations on the organisational environment and infrastructure, to system decommissioning. Other useful guidance can be found in a web publication of the Norwegian data protection authority[95].

75. Effective privacy by design and by default means, in essence, that the protection of individuals' fundamental rights becomes one of the organisation's tasks and as such it should be reflected in their organisational governance and management structure, with proper allocation of privacy tasks and responsibilities, in an accountable way. The main responsibility for privacy requirements stays with the management, implementation may be delegated to the departments responsible for designing and operating relevant systems. The IT and technology departments support the business owners based on their instructions and privacy by design best practices.

76. The role of privacy and data protection officers is central and their involvement is crucial in a privacy by design approach. They need to be in the loop from the early stages when organisations plan systems for the processing of personal data, so that they can support managers, business owners and IT and technology departments as necessary. Their skill set should match these requirements.

77. The EDPS has issued guidelines for IT management and IT governance[96] to support the EU institutions in taking into account privacy and data protection requirements in the development and operation of IT systems, and how the IT governance of an organisation can be established in compliance with the accountability principle. These guidelines are based on generally applicable principles, even though they are targeted to the EDPS specific constituency.

Standardisation efforts

78. Efforts in standardisation have been ongoing to integrate privacy requirements in system design in different standardisation organisations and initiatives[97]. They often take existing approaches to IT security risk management as a model to extend and modify them to privacy risk management. For example, the ISO has issued standards for a privacy framework (ISO/IEC 29100) and a privacy architecture (ISO IEC 29101) related to PII within an information and communication technology environment. Their work includes the extension of the standards ISO/IEC 27001 and 27002 on management of information security to privacy management. Another example is the RFC 6973[98] released by the IETF on "Privacy considerations for Internet Protocols", which aims at the inclusion of privacy requirements in internet protocols.

79. Privacy standardisation is expected to grow also with a view to the role that certifications may have to demonstrate compliance with the GDPR. Specifically, certification

mechanisms may be used to demonstrate compliance with the data protection by design and by default principle[99].

80. In 2015 the EU Commission requested[100] the European Standardisation Organisations (ESOs)[101], which have a cooperation agreement[102] with the Commission, to work on a "privacy and personal data protection by design approach" and "privacy and data protection management framework" for the security industry. In 2017, after the adoption of the GDPR, the ESOs have considered the opportunity for a wider and more articulated work plan integrating privacy, data protection and cybersecurity. It includes: a standard on "Data protection and privacy by design and by default" providing "*requirements for manufacturers and/or service providers*" to implement the principle "*applicable to all business sectors, including the security Industry*" as well as technical reports on specific implementations of the principle[103], initiatives on cybersecurity and privacy and data protection to support recent and ongoing relevant EU level policy making[104]. This standardisation activity may provide a baseline for the industry and all stakeholders for establishing the state of the art in privacy by design. For this reason, it is critical that its outcome will comply with the relevant legal provisions so that it indeed contributes to ensuring proper implementation of data protection by design[105].

4.3 Privacy enhancing technologies

81. Privacy Enhancing Technologies, i.e. specific technological solutions to certain privacy related issues in systems design, have preceded the idea of a comprehensive privacy engineering approach[106] and today they can be considered as quality basic building blocks for engineering privacy. A comprehensive list of existing PETs is beyond the scope of this document, but we can refer to some relevant examples such as a design strategy called "attribute-based credentials", or "anonymous credentials", which give individuals the possibility to authenticate against a service without disclosing their full identity but just selectively disclosing in a trustworthy way only those attributes that are strictly necessary in that context. This is made possible by using specific cryptographic concepts such as zero-knowledge proofs. As an example, if a service is directed to adults, individuals should just disclose securely and reliably that they are older than eighteen without disclosing to the service their age and other identity attributes[107].

82. Many developers, from commercial and non-commercial environments, have invested in providing tools and services with enhanced privacy features. Areas concerned are messaging services, often providing full end-to-end encryption and the absence of any central servers processing or storing communications content or metadata. Their increased popularity, in particular since 2013, has certainly contributed to the adoption of similar encryption standards with more widely used communications tools. Some success has also been observed in areas such as search engines. Popular browsers have added more privacy controls, such as Do Not Track (DNT)[108] features and user control over tracking features, and may be enhanced through many add-ons which suppress tracking attempts or limit profiling. Communication infrastructures, such as Mix networks[109], and also complete operating systems, have also been developed to full usability. The technology oriented elements of the GDPR are triggering new business ideas based on technology, e.g. supporting meaningful consent mechanism and data portability. All these developments demonstrate that the technological competence for privacy by design implementation is available.

83. PETs have developed over the years and efforts have been carried out to make an inventory of what is at disposal, such as ENISA's report on the state of the art of privacy techniques in its publication on privacy by design of December 2014[110]. This report has been complemented by another one on privacy by design for big data analytics[111].

84. In recent years, ENISA has continued to analyse the state of the art and provided a methodology to analyse the readiness and maturity of PETs[112], an approach for assessing online and mobile privacy tools as well recommendations addressed to all stakeholders, from developers to competent authorities, towards creating and maintaining an adequate and qualified PETs maturity repository. In the latest edition of the report, ENISA recommends that competent authorities and regulators promote "*the use of the tool as an online repository of PETs assessments, in the context of the practical implementation of the principle of data protection by design",* that the research community support it by "*actively participating as assessors and users of the platform, as well as encouraging its further use"* and that the research community, the Commission, the EU institutions in the field of security and privacy engage in improving the platform.

85. The EDPS will continue to build upon ENISA's ongoing initiatives through our own future actions to foster privacy engineering. Having a working, up-to-date and quality based assessment tool can contribute to monitoring and benchmarking the level of implementation of privacy by design and by default by being abreast of the state of the art of PETs.

86. In his formal comments[113] on the cybersecurity package of the Commission, the EDPS has pointed out that ENISA is currently the only institution at EU level which has been equipped with the competence and resources to perform dedicated research and advice activities regarding privacy and data protection by design and by default and on privacy enhancing technologies. We repeat our recommendation that this function be maintained and enhanced, if not with ENISA than with another institution, such as the EDPS.

5. Technology for humans: leveraging privacy by design and by default

5.1 Boosting "the state of the art" and the use of privacy enhancing solutions

The current situation

87. The analysis we carried out in 2010 in our "Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy" remains largely valid today. There is a limited uptake of commercial products and services fully embracing the concept of privacy by design and by default. On the other hand, state surveillance revelations have raised awareness of the dangers of ubiquitous and massive collection of personal data for profiling purposes. The arrival of the GDPR has increased public sensitivity and incentivised companies' to shift attention and resources towards privacy and data protection. This trend is likely to continue as the GDPR enters into full application and enforcement actions begin. The current political attention to commercial tracking for the purposes of profiling and targeting may further increase the demand for widely available services and products supporting privacy by design.

88. PETs have made some way into the mainstream commercial offer, including a wider adoption of cryptography for security of personal data (e.g. mobile messaging with end to end encryption), use of Do Not Track[114] and its default no-tracking settings (despite this not

being often honoured and differently interpreted from the service providers) or application of differential privacy algorithms[115] when collecting usage statistics from clients. Privacy friendly search engines appear to operate in a sustainable way. Other services are still in niche offers meeting limited adoption. The family of products and services known as Personal Information Management Systems (PIMS) offer users the possibility to be more in control of their data by encompassing PETs and a new data governance setup, often leveraging new business models. The EDPS has provided an assessment of the state of affairs and recommendations for policy measures with its Opinion on PIMS[116].

89. Academia and industry, with the support of civil society associations and some privacy and data protection authorities have conducted relevant research in fields such as data science, cryptography, quantum physics, artificial intelligence and machine learning as well as human sciences. Engineering and internet associations have started dedicating explicit resources and visibility to privacy engineering[117]. The EU has co-funded many projects through the Framework Programmes for Research and Technological Development and other policy initiatives. This is noticeable and encouraging, yet not enough.

The way forward

90. It is key to keep conducting research and at the same time making sure that privacy technologies can reach a good level of maturity and can be rolled out into affordable technology, products and services in the market.

91. **Policies promoting privacy enhancing technologies and strategies** should be within the priorities of the EU agenda. The LIBE Committee of the European Parliament[118] is debating its opinion on the Commission's Cybersecurity Package. It has taken account of the EDPS urge not to abandon EU support for research and policy advice on PETs and considers changes to the Common proposal for the reviewed ENISA regulation accordingly. We strongly encourage the EU legislator to ensure continued support for privacy enhancing technologies, by clearly allocating tasks and providing adequate resources to an appropriate entity.

92. **A common strategy on privacy by design and PETs can be an outstanding lever for a constructive dialogue also at international level**. The EDPS has launched in recent years the IPEN initiative[119] to bridge the gap between legal requirements and privacy engineering by networking and highlighting existing privacy engineering initiatives and promoting privacy solutions for the public through coordinated actions. While focussed on EU actors so far, in November 2017 we organised a workshop[120] jointly with the Future of Privacy Forum, ULD[121], Carnegie Mellon University and KU Leuven, where we discussed the state of the art and challenges for privacy engineering with a focus on the EU and US. The academic partners decided to carry on research on the issues identified at the workshop and to fill existing gaps in available and affordable privacy technologies in transatlantic[122] cooperation. First academic publications may become available in the near future.

93. **Public administrations should lead by example** in fully embracing the privacy by design and by default principle. We strongly believe this is indeed the way to go, which would indirectly boost an adequate providers' offer. The conclusions of the Tallinn Declaration on eGovernment of October 2017[123] states that "*Development of eGovernment has to respect, support and* enhance *the fundamental freedoms of people such as freedom of expression, privacy and right to the protection of personal data, and comply with relevant EU laws, especially the General Data Protection Regulation. () We will ensure that information*

security and privacy needs are taken into consideration when designing public services and public administration information and communication technology (ICT) solutions, following a risk-based approach and using state-of-the-art solutions...We call upon the Commission to work jointly with our countries to develop proposals on how to take EU research and development funding more into use for the development of cybersecurity and privacy tools and technologies and their deployment in the public administration – in 2018". The EDPS supports this call and will contribute to this policy objective through specific initiatives in its advisory and supervisory role for the EU institutions, where pilot projects could be trailblazers for viable solutions. We call on the Commission to use its funding programs, such as those for research and development, structural funds and administrative cooperation, such as ISA[2], and to coordinate policy initiatives to develop the role of the public sector as a driver to advance the state of the art and the market.

94. A system of policy and economic incentives (the latter in particular for SMEs) should be coordinated at EU and national level to lower the threshold of an economically viable "state of the art" for the benefit of individuals and society at large. This is particularly important in the current data-driven online business landscape where current oligopolies represent an obstacle for start-ups and SMEs to plan worthwhile investments on PETs[124].

95. When choosing technical and organisational measures for data protection, or assessing the measures taken by an organisation, the cost factor plays a role. The benefits organisations enjoy from their investments are balanced against the costs. Not only protecting personal data reduce their risks for liabilities, damages and sanctions. In a society increasingly attentive and alerted on the way the utilisation of their data could have a negative impact on their lives[125], **a convincing and sustained commitment to privacy by design should be considered a competitive advantage**. Deloitte's 2018 Global Human Capital Trend report[126] witnesses a necessary shift of companies towards the "social enterprise", where maintaining positive relationships with diverse stakeholders, including regulators and communities "*is critical to maintaining an organisation's reputation...and to cultivating loyalty among customers*", thus "*influencing its ultimate success or failure*". Protection of individuals' rights and interests through privacy by design and by default can largely contribute to this success key.

96. We **reiterate in particular the call to companies to use their resources, capabilities and creativity to invent new services and business models with the individuals at the centre, in control of their data**[127]. As we stated in our website blog while commenting the ongoing legislative procedure towards an ePrivacy Regulation[128], when referring to complex behavioural advertising practices and underlying technology: "*The limiting factor for effective user control is not the technology. Where the interests of businesses are at stake, we observe tremendous efforts and incredible achievements in the development of technologies*". This shift is essential, to give full substance to the implementation of privacy and data protection by design.

5.2 Privacy by design as a landmark for values driven technology development

97. An increasing number of actors and organisations have launched initiatives aiming at strengthening an element of social and ethical responsibility in the development and roll-out of technologies. While privacy has a central role in these initiatives, it is often pursued in line with other fundamental rights and social objectives.

98. As observed at the CPDP 2018 conference[129], there is a widespread feeling, shared by the Web's inventor[130] and industry insiders[131], that we may have lost control of technology at the service of humanity and society; and that the technology mainstream is rather driven by the business interests of a few companies. It is not just compliance with existing laws, which is at stake, but rather human dignity[132] and our basic fundamental freedoms, including the foundations of our democratic societies. Prevalent business models capitalise on the use of our personal data and the construction of digital representations that reduce ourselves and our personalities to subjects of influence and manipulation. This may heavily impact our lives even when we do not interact online, changing the way we are perceived by others, changing the way we perceive the others and the world around us, and impacting our rights and freedoms.

99. In 2015 the EDPS issued an Opinion[133] on the need to complement the regulatory approach with digital ethics, aiming at supporting the design and use of new technologies in the light of shared human values. The Ethics Advisory Group[134] that was set up has just concluded its two-year mandate and published a final report[135], which analyses main challenges for digital ethics and indicates main directions and risks for the future: the confirmation of the idea that human dignity should remain inviolable in the digital age; that persons and their data are two inseparable concepts; that decision making based on automated big-data profiling may be incompatible with democratic societies and create discrimination; that data commoditisation risks shifting value from persons to personal data.

100. Our call for ethical foundations in technology is shared by other stakeholders, including technology actors, in particular with respect to the expected growth of applications of artificial intelligence and of the role it can play in affecting our lives in many areas. In April 2016 the Institute of Electrical and Electronics Engineers (IEEE) launched a Global Initiative on Ethics of Autonomous and Intelligent Systems[136], an ambitious project for guidance to "*ethical implementation of intelligent technologies*". The goal of the initiative is "*to incorporate ethical aspects of human well-being that may not automatically be considered in the current design and manufacture of A/IS technologies and to reframe the notion of success so human progress can include the intentional prioritization of individual, community, and societal ethical values*". A report collecting input from hundreds of participants throughout the world aims at advancing a public discussion on the topic. Furthermore, working groups have been created to design standards to incorporate ethical considerations in specific contexts including privacy and the processing of personal data by autonomous systems taking decisions without human input[137].

101. Already in 1989 the IETF released a document[138] defining any disruption in the intended use of the Internet as ethically unacceptable, including users' privacy. In October 2017, the IETF provided elaborated guidance on a human rights protocol[139], considered as "*...the first milestone in a longer-term research effort...The Internet isn't value-neutral... This document aims to (1) expose the relationship between protocols and human rights, (2) propose possible guidelines to protect the Internet as an enabling environment for human rights in future protocol development, in a manner similar to the work done for privacy considerations [RFC6973], and (3) increase the awareness, in both the human rights community and the technical community, of the importance of the technical workings of the Internet and its impact on human rights.*".

102. Initiatives supporting the right to privacy can serve as beacons for integrating ethical principles in designing the Internet and the technology-driven society for the complete range

of human rights. The EDPS considers the drive for an effective implementation of the principles of privacy by design and by default as an unprecedented opportunity to boost the respect to ethics in technology. All stakeholders are charged with an important responsibility; in particular companies basing their business on the utilisation of personal data and public authorities, are called to shape their operations to serve the common good.

6. Recommendations and commitments

103. We want to promote a mature and pragmatic debate among stakeholders (policy makers, regulators, industry, academia and civil society) to come out with clear and workable decisions for designing technology at the service of human beings. At the same time, we confirm the EDPS' commitment to an effective implementation of the GDPR and in particular of data protection by design and by default principle. In this context, the EDPS calls on all stakeholders to increase their efforts.

104. The EDPS calls on European Parliament, the Council and the European Commission:

- to ensure strong privacy protection, including privacy by design, in the ongoing legislative process for the **ePrivacy Regulation**; this is both to foster a bigger market for privacy enhanced products and services in communications and to create new market opportunities for European businesses with privacy as part of their organisational DNA;

- to support privacy when adapting or creating legal frameworks which influence the design of technology, by increasing incentives and substantiating obligations, including appropriate liability rules, to integrate privacy by design in products and services, e.g. in the areas of transport, energy, finance, smart cities and IoT;

- to foster the roll-out and adoption of privacy by design approaches and PETs in the EU and at the Member States' level through appropriate implementing measures and policy initiatives;

- to ensure continuous availability of competence and resources for research and analysis on privacy engineering and privacy enhancing technologies at EU level, either by maintaining the current capacity and tasks for ENISA, or by allocating appropriate resources to other entities;

- to support the development of new practices and business models through the research and technology development instruments of the EU, with a special focus on emerging ones such as artificial intelligence, machine learning and the blockchain;

- to support policy initiatives for EU institutions and national public administrations to lead by example and to integrate appropriate privacy by design requirements in public procurement, using policies for cooperation of administrations, and

- to support an inventory and observatory of the "state of the art" of privacy engineering and PETs and their advancement, and to raise awareness on the subject with citizens and economic and political actors.

105. The EDPS will also continue to promote privacy by design, where appropriate in cooperation with other data protection authorities in the EDPB:

- by supporting coordinated and effective enforcement of Article 25 of the GDPR and related provisions, accompanied by adequate awareness raising and other supporting actions, and

- by providing guidance to controllers on the appropriate implementation of the principle laid down in the legal base.

106. We believe that co-ordinating and joining, as possible, technological capabilities among the data protection authorities is essential to promote, define and assess an ambitious "state of the art" for data protection by design and by default. The EDPS invites his colleagues to work together in this direction in the context of the EDPB, as well as the International Working Group on Data Protection and Telecommunications[140] (IWGDPT, "Berlin Group").

107. The EDPS will directly support initiatives and pilot projects for the advancement of privacy engineering and PETs, by leveraging existing initiatives and promoting further co-ordination at EU level and cooperation at international (e.g. transatlantic) level. The IPEN network will be particularly relevant in this regard.

108. Together with the data protection authorities of Austria, Ireland and Schleswig-Holstein, the EDPS has launched a contest[141] for a mobile health app which implements data protection principles.

109. With this Opinion, we want to contribute to mainstreaming the general debate on integrating privacy and ethics requirements in the design of technologies. We welcome feedback to this preliminary Opinion. The 2018 International Conference of Privacy and Data Protection Commissioners[142], jointly organised by the EDPS and the Bulgarian data protection authority, should be a milestone in the discussion about a digital ethics in general and an opportunity to better define the way forward for privacy by design, as a good example of a value-driven approach towards technology development.

Brussels, 31 May 2018

Giovanni Buttarelli

European Data Protection Supervisor

Notes

[1] EP President Tajani invites Facebook CEO: http://www.europarl.europa.eu/news/en/agenda/briefing/2018-04-16/1/facebook-meps-to-discuss-misuse-of-eu-citizens-personal-data.

[2] US Senate Committee hearing of Facebook CEO: https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Zuckerberg%20Testimony.pdf.

[3] UK House of Commons Digital, Culture, Media and Sports Committee: Investigation on fake news: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/.

[4] German Federal Parliament, Digital Agenda Committee, report https://www.bundestag.de/presse/hib/2018_03/-/548624.

[5] Resolution French Parliament, http://www.assemblee-nationale.fr/15/pdf/propositions/pion0858.pdf.

[6] The Special Eurobarometer 431 survey published in June 2015 reported that more than eight out of ten respondents feel that they do not have complete control over their personal data. Among these 31 % believed they had no control at all. (http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf) This perception has been recently confirmed by other studies carried out by other organisations. For example, PwC surveyed 2000 Americans in 2017: https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/cybersecurity-protect-me.html. Only one out of ten respondents declared they felt they were in complete control of their personal data.

[7] Giovanni Buttarelli on CNN, 5 April 2018: http://transcripts.cnn.com/TRANSCRIPTS/1804/05/qmb.91.html.

[8] EPDS Opinion 3/2018 on online manipulation and personal data of 19 March 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[9] 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, 04.05.2016, p.1.

[10] Directive 95/46 of the European Parliament and 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.

[11] Tim Berners-Lee, Three challenges for the web, according to its inventor, Web Foundation · March 12, 2017, https://webfoundation.org/2017/03/web-turns-28-letter/.

[12] Tim Berners-Lee, The web is under threat. Join us and fight for it. Web Foundation · March 12, 2018, https://webfoundation.org/2018/03/web-birthday-29/.

[13] Pacemaker data was used in at least one court case in order to verify whether the heart rate recordings were consistent with the suspect's account of events. https://www.forensicmag.com/news/2017/02/data-suspects-pacemaker-leads-arson-insurance-fraud-charges.

[14] There is ample research on the effectiveness of environmental legislation. The conclusion that "*with near certainty (...) environmental regulations drove the technological improvements that allowed for increased manufacturing output with decreased emissions*" is supported, e.g. by Bryan C. Williamson, Do Environmental Regulations Really Work?, in: University of Pennsylvania, The Regulatory Review, 24 November 2016, https://www.theregreview.org/2016/11/24/williamson-do-environmental-regulations-really-work/.

[15] Melvin Kranzberg, Technology and History: "Kranzberg's Laws", in : Technology and Culture, Vol. 27, No. 3 (Jul., 1986), pp. 544-560.

[16] Ibid.

[17] See: https://edps.europa.eu/data-protection/our-work/ethics_en

[18] 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, 04.05.2016, p.1.

[19] See e.g.: Lina Jasmontaite, Irene Kamara, Gabriela Zanfir-Fortuna and Stefano Leucci, "*Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules*" EDPL Vol. 4 (2018), forthcoming.

[20] Data protection authorities and their organisations (WP29, EDPB) will provide appropriate guidance on implementation of the GDPR provisions.

[21] See for example *Tsormpatzoudi, P., Berendt, B., & Coudert, F. (2016). Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, &*

S. Schiffner (Eds.), Privacy Technologies and Policy. Third Annual Privacy Forum, APF 2015. Luxembourg, Luxembourg, October 7-8, 2015. Revised Selected Papers (pp. 199-212). Berlin etc.: Springer. LNCS 9484. © Springer:

https://people.cs.kuleuven.be/~bettina.berendt/Papers/tsormpatzoudi_berendt_coudert_APF2015_with_bib_metadata.pdf.

[22] Two examples of solutions proposed are exposed in the following papers: "*Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84–88, 1981*" and "*Security without identification: transaction systems to make big brother obsolete. Commun. ACM, 28(10):1030–1044, October 1985. http://doi.acm.org/10.1145/4372.4373.*".

[23] This paradigm was called "multilateral security" and can be originally found in papers such as "*Kai Rannenberg. Recent development in information technology security evaluation – the need for evaluation criteria for multilateral security. In Richard Sizer, Louise Yngström, Henrik Kaspersen, and Simone Fischer-Hübner, editors, Security and Control of Information Technology in Society – Proceedings of the IFIP TC9/WG 9.6 Working Conference. North-Holland Publishers, 1994.*".

[24] One of the most adopted definitions of the term "Privacy Enhancing Technology" was given by Borking, Blarkom and others in 1995, calling them "*a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system*".

[25] See e.g.; "The Guardian - Revealed: how US and UK spy agencies defeat internet privacy and security": https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[26] "The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual", from IETF website: https://www.ietf.org/about/who/.

[27] "IETF news- Security and Pervasive Monitoring", 7 September 2013: https://www.ietf.org/blog/security-and-pervasive-monitoring/.

[28] See: https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf. The "seven foundational principles" are: 1. Proactive not Reactive, Preventative not Remedial; 2. Privacy as the Default Setting; Privacy Embedded into Design; 4. Full Functionality — Positive-Sum, not Zero-Sum; 5. End-to-End Security — Full Lifecycle Protection; 6. Visibility and Transparency — Keep it Open; 7. Respect for User Privacy — Keep it User-Centric.

[29] European Parliament and the Council, 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 OJ L 281, 23.11.1995.

[30] See: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.

[31] The WP29 was composed by representatives of all the EU/EEA data protection supervisory authorities. It is based on the provisions of Article 29 of Directive 95/46/EC. It has been replaced with the EDPB by the GDPR.

[32] The Opinion can be found here: https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_en.pdf.

[33] ***Data protection by design and by default***

1.Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

[34] While the terms "privacy" and "data protection" are used with different meanings in the EU legal framework, we will use the expression "privacy by design and by default" to comprise also any uses of the "data protection by design and by default" expression. Furthermore, when we just refer to "privacy by design", this does not exclude "privacy by default" but just emphasises the "design" dimension.

With a reference to the Charter of Fundamental Rights of the EU, "privacy" is normally used to describe the right expressed by Art.7 ("Respect for private and family life") whereas "data protection" is used for Art.8 ("Protection of personal data").

[35] The GDPR defines the controller as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data ...*" See Article 4.

[36] These certification mechanisms must be approved based on Article 42. An interpretation of this Article has been adopted by the European Data Protection Board (see Article 70 of the GDPR).

[37] Article 5 lists all principles relating to the processing of personal data. They are called: a) lawfulness, fairness and transparency; b) purpose limitation; c) data minimisation; d) accuracy; e) storage limitation; f) integrity and confidentiality. For more detail, please read the whole Article.

[38] In this document, the terms "safeguard" and "measure" are used interchangeably.

[39] In general, in project management literature, the "implementation/construction" of the project/system, following the design and preceding its operation, and the "dismissal/transition" of a project/system following its operation are also noticeable project phases with their own specific requirements. Nevertheless there are no reasons to believe that the legislator did not want to refer to the whole lifecycle of a project by just mentioning the design and operational phases.

[40] For examples of the fundamental rights and freedoms to protect, Recital 75 of the GDPR represents a valuable and authoritative source.

[41] In reality one example is given to clarify the concept, where "pseudonymisation" is mentioned as a possible safeguard to meet the "data minimisation" principle.

[42] See definition of « data subject » in Article 4 (1) of the GDPR.

[43] The data purpose limitation and minimisation principles are described respectively in Article 4(1) (b) and (c).

[44] See also the "EDPS Opinion on the data reform package" of 7 Match 2012, in particular paragraph 180. Of course, this Opinion referred to the original EC proposal COM/2012/011 final: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011 . The formulation of the principle of privacy by default in the original proposal is very close to that of the final text.

[45] For example, if I use an app for car sharing I expect that my location is used for me to know where the closest car is parked and that my contact details be used to get in touch with me in the context of the service . This does not mean that, by default, my location and contact details should be sent over to local bike sellers to send me advertising and offers.

[46] See definition of « processor » in Article 4 (8) of the GDPR.

[47] See Article 28(1) of the GDPR.

[48] The "recitals" of a legal text precede the list of the articles ("substantive provisions"). Their purpose is to give background and rationale of the articles and provide relevant additional recommendations and explanations. Even though only the articles are legally binding, nonetheless recitals are often used to interpret the law, including by regulatory bodies and courts.

[49] The rules of Article 35 of the GDPR have been complemented by relevant Guidelines on Data Protection Impact Assessment (DPIA) - wp248, issued by the Working Party 29 and available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[50] See how this concept is developed in the "EDPS provisional guidance on documenting processing operations for EU institutions, bodies and agencies": https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en, in particular Part 1.

[51] Op. cit. in endnote 49.

[52] See (Articles 35(1) and 35(10), and recitals 90 and 93 of the GDPR).

[53] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p.37; amended by Directive 2009/136/EC.

[54] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. OJ L 91, 7.4.1999, p. 10.

[55] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, OJ L 153, 22.5.2014, p. 62. This is also referred to as the Radio Equipment Directive.

[56] EDPS "Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)", April 2017, p. 19: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf.

[57] Commission 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications)' COM(2017) 10 final, 2017/0003 (COD).This proposal is currently undergoing the EU ordinary legislative procedure.

[58] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73.

[59] EIDAS Regulation, Article 12 (3) (c).

[60] Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems (OJ L 73, 13.3.2012, p. 9):

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012H0148&from=EN.

[61] Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (OJ L 300, 18.10.2014, p 63):

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014H0724&from=EN. The industry tested the DPIA Template for two years and the Commission made an assessment of the test phase. The Template is now being finalised follow-ing up the results of the assessment, also with a view to the new GDPR requirements.

[62]See: https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp4_bref_smart-metering_systems_final_deliverable.pdf.

[63] The BAT concept was inherited from the industrial sector where used in the policy for the reduction of gas emissions: https://www.eea.europa.eu/themes/air/links/guidance-and-tools/eu-best-available-technology-reference.

[64] See endnote 28.

[65] See endnote 30.

[66] See for example proposals in Canada: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/news-release/9691065 and in Brazil: https://iapp.org/news/a/brazilian-general-bill-on-the-protection-of-personal-data/.

[67] See e.g. the Office of the Victorian Information Commissioner: https://www.cpdp.vic.gov.au/menu-privacy/privacy-organisations/privacy-organisations-privacy-by-design.

[68] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers": https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[69] The others are "simplified choice" and "transparency".

[70] Remarks of Commissioner Edith Ramirez, Privacy by Design Conference, Hong Kong, June 13, 2012: https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf. The Fair Information Practice Principles (FIPPs), were adopted by US government for federal agencies when processing PII. They could be basically summarised in: transparency, use limitation, access and correction, data quality, and security. Many consider the FIPPs as the original building blocks for worldwide privacy laws and charters, including in the EU.

[71] See endnote 70.

[72] See https://www.ftc.gov/about-ftc.

[73] From the same source quoted in endnote 70: "*The FTC advocates these concepts as best practices for companies to adopt now on a voluntary or self-regulatory basis. We have also called on the U.S. Congress to enact comprehensive privacy legislation that draws on the ideas in the FTC's framework*".

[74] "NISTIR 8062 - An Introduction to Privacy Engineering and Risk Management in Federal Systems":

https:/doi.org/10.6028/NIST.IR.8062.

[75] From the source in endnote 74 : "In *July 2016, the Office of Management and Budget (OMB) released an update to Circular No. A-130 that requires agencies to apply the NIST Risk Management Framework (RMF) in their privacy programs. That OMB update also includes a new emphasis on managing privacy risk beyond solely compliance with privacy laws, regulations and policies. Although agencies should already be using PIAs to address privacy risk, it is more difficult for them to do it consistently in the absence of a model that enables a*

repeatable and measurable process to assess privacy risk. Repeatability is important so that the process can be performed consistently over time (not that the outcome is necessarily the same each time). Measurability matters, so that agencies can demonstrate the effectiveness of privacy controls in addressing identified privacy risks.".

[76] https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering.

[77] For Fair Information Practice Principles see endnote 70.

[78] See: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[79] For an idea on software development methodologies see: https://en.wikipedia.org/wiki/Software_development_process.

[80] For an idea of non-functional requirements see: https://en.wikipedia.org/wiki/Non-functional_requirement.

[81] The exception is when the main purpose of the system is managing privacy features (e.g. a browser plug-in to avoid being tracked).

[82] "Privacy and Data Protection by Design – from policy to engineering", ENISA, December 2014: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

[83] "Protection Goals for Privacy Engineering", Marit Hansen, Meiko Jensen and Martin Rost, 2015 IEEE CS Security and Privacy Workshops.

[84] For an idea on information security properties see : https://en.wikipedia.org/wiki/Information_security.

[85] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management", 2010.

[86] See endnote 74.

[87] PII stays for Personally Identifiable Information. In "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", NIST Special Publication 800-122, April 2010: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf, PII is defined as "*any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information*". PII should not confused with "personal data" as defined in Article 4(1) of the GDPR.

[88] In this case the principles of reference are the Fair Information Practice Principles (see endnote 54).

[89] See endnote 74, in section 3.1.1.

[90] See https://distrinet.cs.kuleuven.be/software/linddun/. The methodology comes from the DistriNet research group of the KU Leuven University.

[91] A design pattern "provides a scheme for refining the subsystems or components of a software system, or the relationships between them. It describes a commonly recurring structure of communicating components that solves a general design problem within a particular context." as originally defined in late 1970's.

[92] An example of catalogue of patterns can be found here : https://privacypatterns.eu.

[93] See e.g. Michael Colesky, Jaap-Henk Hoepman, Christiaan Hillen, "A Critical Analysis of Privacy Design Strategies": https://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf.

[94] PRIPARE Handbook - Privacy and Security by Design Methodology: http://prepareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf.

[95] Datatilsynet, "Software development with Data Protection by Design and by Default": https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/.

[96] EDPS "Guidelines on the protection of personal data in IT governance and IT management of EU institutions", March 2018: https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf.

[97] See a list (non exhaustive) of privacy related standardisation initiatives in IPEN wiki: https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards#Privacy_Standards.

[98] See: https://tools.ietf.org/html/rfc6973.

[99] See endnote 36.

[100] European Commission (2015) M/530 Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive

95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy: http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548.

[101] See: https://ec.europa.eu/growth/single-market/european-standards/key-players_en.

[102] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025.

[103] Presentation at CEN/CENELEC Cybersecurity Conference, 12 March 2018, A. Guarino, K. Rannenberg: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/GUARINO_RANNENBERG_CEN-CLC_JTC8.pdf.

[104] See: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Walter-FUMY_Chair_CEN-CLC_JTC13.pdf.

[105] See also Kamara, I., "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", in European Journal of Law and Technology, Vol 8, No 1, 2017: http://ejlt.org/article/view/545/723#_edn20.

[106] The Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies is awarded to outstanding Research in PETs. https://petsymposium.org/award/index.php.

[107] See https://privacybydesign.foundation/en/ (IRMA project): https://privacybydesign.foundation/irma-explanation/ for an application of the technique.

[108] The DNT feature as implemented in web clients sends the website a signal communicating that the client does not want to be tracked. The W3C has carried out a standardisation initiative called Tracking Preference Expression, which can be found at: http://www.w3.org/2011/tracking-protection/.

[109] Mix networks are communication protocols designed in a way to make tracing back senders and receivers of messages a very difficult task. See, for example "George Danezis, University of Cambridge, Technical Report n° 594, 2004 - Designing and attacking anonymous communication systems":

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-594.pdf.

A Wikipedia entry exists, you might want to consult: https://en.wikipedia.org/wiki/Mix_network.

[110] See endnote 82.

[111] Privacy by design in big data", ENISA, December 2015: https://www.enisa.europa.eu/publications/big-data-protection.

[112] ENISA work on PETs can be found in here : https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies.

[113] Formal comments of the EDPS on the Cybersecurity package, 15 December 2017, https://edps.europa.eu/data-protection/our-work/publications/comments/cybersecurity-package_en.

[114] See endnote 108.

[115] Differential privacy is a process that introduces some "noise" in the personal data collected so that they cannot be related to identifiable individuals while ensuring a certain level of accuracy in computations (e.g. statistics) produced from those data. See an example of application in widely used products: https://images.apple.com/privacy/docs/Differential_Privacy_Overview.pdf. References to commercial products does not imply EDPS endorsement.

[116] EDPS Opinion on Personal Information Management Systems, October 2016: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

[117] As an example of this: the IEEE has started siding its Symposium on Security & Privacy with an International Workshop on Privacy Engineering: http://www.ieee-security.org/TC/SPW2017/IWPE/program.html.

[118] Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Industry, Research and Energy on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM(2017)0477–C8-0310/2017(COD)): http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-615.394&format=PDF&language=EN&secondRef=02.

[119] See: https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en.

[120]See https://fpf.org/2017/08/30/privacy-engineering-research-gdpr-trans-atlantic-initiative/.

[121] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

[122] See panel at CPDP 2018: https://www.youtube.com/watch?v=3S0CV2ujIVM.

[123] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017 http://ec.europa.eu/newsroom/document.cfm?doc_id=47559.

[124] The EDPS is contributing in this direction in particular through the Digital Clearinghouse Initiative: https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en.

[125] You might want to read this reaction over the recent Facebook-Cambridge Analytica affair: https://www.theguardian.com/technology/2018/apr/12/facebook-how-to-quit-delete-account-addiction-what-to-do.

[126] You can find the report at: https://www2.deloitte.com/content/dam/insights/us/articles/HCTrends2018/2018-HCtrends_Rise-of-the-social-enterprise.pdf.

[127] See EDPS Opinion on Personal Information Management Systems (endnote 116) and in particular section 3.9.

[128] See: https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy_en

[129] See: https://edps.europa.eu/sites/edp/files/publication/18-01-25_privacy_by_design_privacy_engineering_cpdp_en_3.pdf.

[130]See e.g. : http://www.wired.co.uk/article/is-the-internet-broken-how-to-fix-it.

[131] See e.g.: https://www.theguardian.com/technology/2018/jan/13/mark-zuckerberg-tech-addiction-investors-speak-up.

[132] Article 1 of the EU Charter of Fundamental Rights: "*Human dignity is inviolable. It must be respected and protected*".

[133] EDPS Opinion Towards a new digital ethics Data, dignity and technology, December 2015: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf.

[134] See endnote 26.

[135] https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[136] See: http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html.

[137] See: https://ethicsinaction.ieee.org/.

[138] IETF RFC 1087 "Ethics and the Internet": https://tools.ietf.org/html/rfc1087.

[139] IETF RFC 8280 "Research into Human Rights Protocol Considerations": https://trac.tools.ietf.org/html/rfc8280.

[140] IWGDPT working papers are available at https://www.datenschutz-berlin.de/working-paper.html.

[141] https://edps.europa.eu/data-protection/our-work/ipen/edps-ipen-privacy-design-contest-mobile-health-mhealth-applications_en

[142] See: https://edps.europa.eu/press-publications/press-news/press-releases/2017/2018-international-conference-data-protection-0_en.