Recommendations on shaping technology according to GDPR provisions

Exploring the notion of data protection by default

DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Contributors

Marit Hansen (DPA Schleswig-Holstein), Konstantinos Limniotis (Hellenic DPA)

Editors

Athena Bourka (ENISA), Prokopios Drogkaris (ENISA)

Acknowledgements

We would like to thank Giuseppe D'Acquisto (Garante), Ailo Krogh Ravna (Forbrukerradet) and Gro Mette Moen (Forbrukerradet) for reviewing this report and providing valuable comments.

ISBN 978-92-9204-285-1, DOI 10.2824/518496

Table of Contents

Executive Summary

The choice of defaults in software engineering is not a new concept, as developers have to deal with the question of appropriate pre-settings of information and communication technology all the time. However, the principle of "data protection first", as demanded by the General Data Protection Regulation (GDPR) when it comes to data protection by default, has neither been the standard behaviour of products, services and applications nor a regular principle in software design methods.

Indeed, GDPR in its Article 25(2) asks for data-protection-friendly pre-settings in a way that only the minimum amount of personal data are processed, the extent of the processing is minimal, the shortest period of storage is chosen, and the possibilities for accessing the personal data are minimised as well. Thus, the objective of data protection by default is to ensure the fundamental principles of data minimisation and storage limitation in the IT systems – at least in the beginning when the user has not changed the pre-installed settings -, taking always into consideration the specific purpose and the overall context of the processing of personal data. This contributes to the GDPR's goal of fairness of processing personal data. It can also contribute to other important GDPR provisions, such as the security of personal data processing.

This report aims to shed some light on what the data-protection-by-default principle means in information technology design, what is the situation today, as well as how the new GDPR obligation could support controllers in selecting data-protection-friendly defaults. Still, several aspects of the data protection by default will have to be discussed more thoroughly in the future, and appropriate best practice solutions should be made more visible. Analysing the interplay between data protection and security defaults is also essential to this end, taking into consideration relevant usability aspects.

To this end, the main recommendations made in the report for all relevant stakeholders are presented below.

Recommendations for data controllers and producers of products, services and applications

The GDPR demands that data controllers realise data protection by design and by default in their data processing or, otherwise build their processing on the principle of "data protection first". Producers of products, services and applications, although not having a direct obligation under GDPR, should support controllers to reach this essential requirement with proper design, guidance and tools.

Data controllers should make the notions of 'by design' and 'by default' key building blocks of their data processing operations and invest in relevant best practice implementations.

Producers of products, services and applications should refrain from using design patterns that can lead users towards non-privacy friendly choices; On the contrary, they should embed security, as well as data protection by design and default into their business models and provide adequate guidance and support to data controllers and end-users.

Recommendations for end-users

As products, services and applications do not always embed data protection by default, end-users cannot in all cases rely on a data protection friendly pre-setting (and sometimes not even on a secure pre-setting).

End users should seek to understand the security and data protection options and configurations of the products, systems or applications they use; they should inform themselves about their rights under the data protection (as well consumer protection) legislation.

Recommendations for regulatory bodies

The supervisory authorities should clarify their expectations on how to translate the requirement of data protection by default into action. A more detailed interpretation of the provisions in the GDPR could significantly support controllers in the design and adoption of data protection friendly defaults.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should provide further guidance on the notion and practical implementations of defaults; they could also present best practice examples and relevant use cases that can be used by the data controllers (as well as the producers of products, services and applications) who seek to meet the GDPR requirements.

Recommendations for policymakers and standardisation bodies

The principle of data protection by default should be considered by lawmakers and standardisation initiatives when it comes to the processing of personal data. In the interest of clarity, legal and technical norms should be explicit on default settings, whenever this is applicable. The interplay with security defaults is also essential to consider to this end.

Policy makers and standardization bodies should support the adoption of the data protection by default (as well as by design) by proposing, wherever possible, relevant technical norms and solutions, as well as considering its correlation with the notion of security by default.

Recommendations for the research community

For researchers, the data-protection-by-default debate provides multiple interesting angles, including open questions on the definition of pre-settings, as well as the notion of the principle of “data protection first” in relation to other fundamental design principles, such as security and usability.

The research community should continue working on the notion of data protection by default, especially in correlation with security and usability, as well as other interdisciplinary principles that govern defaults; they should also analyse new online business models based on security and privacy defaults, as well as technologies that can facilitate their adoption.

1. Introduction

1.1 Background

When designing IT systems or IT-based services, the default settings, i.e. the properties and functionalities that are in place at the very first employment (of these systems or services) without requiring any activity or choice by the user, are of vital importance, as they constitute the basis upon which the user will initiate his or her interaction. Indeed, the default determines at least the first usage and, if users are not able or willing to change it, it further determines the ongoing use. This crucial characteristic of default settings ("defaults") is also relevant to security and data protection related properties and functionalities and can be essential to the risk for the rights and freedoms of individuals.

Recognizing the role of defaults in the protection of personal data, the General Data Protection Regulation (GDPR) [1] provides under its Article 25(2) a new obligation for data controllers[2] with regard to data protection by default. In particular, it mandates that the controller, by the use of appropriate technical and organisational measures, shall ensure that only personal data that are necessary for the purpose are processed. This is applicable to the amount of the personal data collected, the extent of their processing, the period of storage and their accessibility. Moreover, the controller shall ensure that by default personal data are not made accessible, without the individual's intervention, to an indefinite number of natural persons.

The obligation for data protection by default is closely interlinked with the one on data protection by design stipulated in Article 25(1) GDPR, which states that the controller shall implement appropriate technical and organisational measures designed to implement the data protection principles of GDPR in an effective manner and integrate the necessary safeguards into the processing of personal data. In fact, data protection by default could be seen as a natural extension of data protection by design when it comes to choosing the data protection friendly default settings. Together, data protection by design and by default, fall within the overall notion of privacy engineering, i.e. embedding privacy requirements into the information systems' design and operation. In this way, data protection by design and by default, are also closely interlinked with security of processing (article 32 GDPR), which is another essential GDPR requirement.

While data protection by default might be perceived only as a substantiation of data protection by design, the task of selecting and implementing the default settings has its own specific significance and challenges. Indeed, choosing the defaults is not trivial, even with security and data protection by design in mind, as it requires an assessment of the necessity for each purpose of the processing, balanced with other equally important requirements, such as usability and expected behaviour of the system or service. At the same time, it appears that default settings in modern systems and services are not always respecting the data protection principles, while in certain cases there are even patterns of nudging users towards non-privacy friendly choices[3], which can often lead to extensive users' tracking[4].This shortcoming seems to be

[1] Regulation (EU) 679/2016 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), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

[2] The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means for the processing of personal data.

[3] See 2018 report of the Norwegian Consumer Council, 'Deceived by design', which discussed how companies use "dark patterns" to discourage users from exercising their rights to privacy [Forbrukerrådet, 2018].

[4] See also relevant report of Norwegian Consumer Council "Every Step You Take" [[Forbrukerrådet, 2018 -1].

prominent in the area of mobile apps, where several entities (app developers, operating system –OS- providers, library providers, app stores, etc.) are involved in the processing of personal data, while users are often unaware about what their default settings are and how they can modify them.[5]

Against this background and following previous ENISA's work in the field [ENISA 2014] [ENISA, 2015], the Agency decided under its 2018 work-programme[6] to explore further the notion and possible application of data protection by default. As ENISA is expected to provide guidance on aspects of network and information security policy in the EU, it is logical that addressing particular areas of interest, including in privacy and data protection, is a reasonable extension of its work and it meets stakeholders' needs. Indeed, given the close interplay between the defaults and the 'by design' principle, as well as the security of personal data, ENISA perceives this study as the first step to open the discussion towards the critical role of defaults in online services and applications, both for the security and privacy of users.

1.2 Scope and objectives

The scope of this report is to discuss the concept of data protection by default in GDPR and further analyse its main elements and possible implementation aspects.

In particular, the report has the following objectives:

- Explore the notion of data protection by default and the relevant new obligation for data controllers under GDPR.
- Examine the specific criteria that can be useful for the definition of data protection friendly defaults.
- Provide relevant examples and best practices in the field.

Overall, the report aims at contributing to the notion of data protection defaults, as a starting point for the overall discussion for security and privacy defaults in online systems and services.

The target audience are data controllers, producers of products, services and applications, Data Protection Authorities (DPAs), researchers, as well as any other party interested in the notion of data protection by default.

It should be noted that the discussion and examples presented in this report are only focused on analysing the ideas around data protection by default; they should by no means be interpreted as a legal opinion on the relevant cases.

1.3 Outline

The structure of the report is as follows:

- Chapter 2 explores the notion of data protection by default and further elaborates on the GDPR relevant provision and its main elements.
- Chapter 3 presents some best practices on the practical application of data protection by default.
- Chapter 4 proposes a list of self-assessment questions that may be of use for controllers or producers of products, services and applications when determining the default settings.
- Chapter 5, summarizing the previous discussions, provides the main conclusions and recommendations for all related stakeholders.

[5] See also relevant ENISA's study on privacy and data protection in mobile applications [ENISA, 2017].
[6] ENISA programming document 2018-2020, https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020.

This report is part of ENISA's work in the area of privacy and data protection[7], which focuses on technical solutions for the implementation of GDPR, privacy by design and security of personal data processing.

[7] https://www.enisa.europa.eu/topics/data-protection

2. Exploring data protection by default

In this Chapter, we explore the concept of "data protection by default". In particular, after a short definition of the notion of defaults in Section 2.1, Section 2.2 discusses the importance of default settings in system design. Section 2.3 then describes the view of the GDPR where Article 25 defines requirements both for data protection by design and by default. The implementation of data protection by default is further analysed in Section 2.4, where a number of parameters are presented with regard to selecting data protection friendly default settings. This is important both for data controllers, as well as for producers of products, services and applications who should be considering data protection by default when developing IT systems and IT-based services. Section 2.5 concludes this Chapter by briefly introducing the notion of security by default and linking it to the scope of this study.

2.1 The meaning of default settings

In the process of building IT systems or IT-based services, the developers have to decide on the possible ways of implementing the desired functionality. To this end, some functions are "wired in", i.e. they cannot be configured or changed after the system/service has been built. For other functions, it depends on the configuration, i.e. the specification of the system's relevant settings, whether or not these functions are activated and which parameters are used. This configuration can be adapted according to the needs of the users. For instance, the end-users themselves may define the desired settings and potentially change them over time, or a company may enforce the appropriate configuration for all employees' IT systems before the role-out phase.

Regarding the configurable functions, the developers have to determine which of them should be pre-configured, i.e. set to specific values, which represent the *default* behaviour of the IT system in case nobody changes these settings. Alternatively, it could be refrained from pre-selecting any configuration; e.g. when installing the IT system or service, the users (or local administrators) could be asked for their choices, thereby configuring the system according to their needs.

To this end, the default in an IT system or service refers to a pre-configured or pre-set value that is assigned to a configurable setting of this system or service. This setting will not change without the user's intervention. It can vary from a single selection to multiple selections regarding the same function, which all together formulate the so called 'default settings'. Moreover, it can be relevant to the core system functionality or the provision of complementary or additional system functions.

Defaults govern a great part of the daily usage of IT systems and services, which may or not be evident to users. For example, default settings for network mode, system display, backup options, internet browser, are only a few typical cases, which are applicable to all types of IT operating systems. Default values are often pre-configured in several online forms, when users are asked to provide information (e.g. defaults on country or language selection). Security defaults determine the basic security properties that a service or application provides (e.g. with regard to access to a computer's resources or storage of information). Privacy defaults determine the default way an application or device processes the personal data of its user (e.g. with regard to access to contact data, camera or microphone use, location data, etc. in a mobile phone).

Whenever a default is assigned, the user's interaction is clearly minimised. Therefore, defaults are essential in order to allow the smooth operation of systems and services without burdening the users with a multitude of questions and choices to make. At the same time, using defaults may increase errors on the users' side, i.e. if defaults are not appropriately selected or if the users are not adequately informed. For this reason, the possibility of changing the defaults is an indispensable requirement that goes together

with offering the default option in the first place; in certain cases it might even be required to change the defaults upon first use (e.g. default password in a server's configuration). In all cases, the availability of information about the defaults is of utmost importance for proper utilisation of the full functionality of a system or service.

2.2 The importance of data protection defaults in system design

Defaults play an important role in system design. As mentioned earlier, the default setting determines how the system works if nothing is changed. Thus, it is not only the starting point of how the system is used, but since many users will never change the default setting, it will govern the usage to a great extent [Kesan, 2006].

This holds for privacy and data protection, too. When Cavoukian developed the foundational principles for privacy by design, she dedicated one principle to *"Privacy as the default setting: 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."* [Cavoukian, 2011]. Perhaps it is questionable whether there is such thing as a guarantee for *"intact privacy"* in real-life situations. The European Data Protection Supervisor elaborated on the default principle in the opinion on the Data Protection Reform Package: *"The idea behind the principle is that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it. The data subject should in principle be left the choice to allow use of his or her personal data in a broader way."* [EDPS, 2012, p. 29-30].

Either way, the gist of this basic principle is convincing: Certainly, current systems and services very often do not implement anything near privacy-enforcing defaults [Forbrukerrådet, 2018]. Instead, common defaults are rather privacy-infringing, e.g. if users are not asked for consent (opt-in), but have to object (opt-out) if they don't agree with the processing of their personal data [Johnson, 2002].[8] A lack of awareness, potentially high effort for opting out and insufficient usability make it hard for users to maintain their privacy, or at least to reduce the data protection risk [Leon, 2012].

In addition to the opt-in vs. opt-out questions, researchers have investigated how the way of presenting the choices to the user, that are offered on the basis of the default, influences the behaviour [Acquisti , 2011 and Keller, 2011]. The concept of nudging can be based on the pre-configured defaults [Thaler, 2008]. While nudging often maybe suspected as manipulative, the information of choices can be enriched by comparing different options and highlighting the benefits and losses of the alternative choice (so-called "enhanced active choice", [Keller, 2011].

For the European market of processing of personal data, the GDPR has defined the principle of "data protection by default" in Article 25 as a technology-perspective substantiation of the well-known – but not yet well implemented – necessity principle. The GDPR acknowledges the power of system design and demands appropriate defaults that put data protection first and ensure that only data processing to the minimum extent necessary for a purpose takes place.

2.3 The notion of "data protection by default" in GDPR

2.3.1 Article 25 GDPR

Data protection by design and by default is regulated in Article 25 GDPR that contains three paragraphs: While the first paragraph tackles data protection by design, the second paragraph describes the requirements for data controllers for data protection by default, and the third paragraph refers to certification (cf. Article 42 GDPR) as an element to demonstrate GDPR compliance. Article 25 GDPR is

[8] The GDPR makes it very clear that "pre-ticked boxes or inactivity should not [...] constitute consent", cf. Recital 32.

central for the accountability principle defined in Article 5(2) GDPR and substantiated in Article 24 GDPR, where it is made clear that the data controller has to be able to demonstrate that processing is performed in accordance with the GDPR. This includes how the processing is designed and whether the appropriate technical and organisational measures are being implemented.

Focusing in this text on data protection by default, Article 25(2) GDPR reads as follows:

"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."

2.3.2 Data-protection principles addressed by data protection by default

Data protection by default implements the rule to limit the data processing to what is necessary for its purpose, namely the data protection principles of data minimization (Article 5(1)(c) GDPR) and storage limitation (Article 5(1)(e) GDPR) on the basis of the principle of purpose limitation (Article 5(1)(b) GDPR). Although its main focus is on necessity, Article 25(2) is also linked to other data protection principles, such the principle of transparency (Article 5(1)a GFPR), as well as the principle of integrity and confidentiality (Article 5(1)(f)GDPR) and the overall security of processing according to Article 32 GDPR (see also relevant discussion in Section 2.5).

Data protection by default is tightly interlinked with data protection by design, demanded by Article 25(1) GDPR: *"implement appropriate technical and organisational measures [...] which are designed to implement data-protection principles"*. While the first paragraph of Article 25 GDPR requires building in each of the data-protection principles laid down in Article 5 GDPR, the second paragraph is dedicated to a data-protection-friendly default setting, focusing on those data-protection principles related to necessity. The focal point for determining the necessity is *"each specific purpose of the processing"*. Thus, data protection by default does not force the deactivation of any lawful processing, but it requires the limitation of the processing to the minimum depending on each specific purpose.

It should be stressed that, while data protection by default directly refers to the GDPR data protection principles (Article 5 GDPR), it introduces a very important novelty, i.e. putting the choices and needs of individuals as the starting point for any processing of personal data. Indeed, by setting data protection defaults, the controller, being as neutral as possible, is actually making the individuals' expectations (for the processing of personal data) a core requirement, thus also considerably contributing towards building trust between controllers and individuals. This also shows the dynamic nature of defaults, as well as the fact that they may significantly vary between different types of personal data processing.

2.3.3 Different roles with regard to data protection by default

Following the GDPR terminology, the different parties/roles involved in the implementation of data protection by default are as follows:

- The **producer** (of a product/service/application) decides on the design and on the configuration options of a product, service or application.
- The **data controller** determines the purposes and means of the processing of personal data (Article 4(7) GDPR). The data controller is responsible for the data processing including the default pre-setting (as offered by the producer's product, service or application).
- The **data processor** processes personal data on behalf of the data controller (Article 4(8) GDPR).

- The **data subject** is a natural person, or otherwise an **individual**, whose personal data are processed. A data subject can be a **user** or a non-user.
- A **user** (of a product/service/application) is an individual using a product, service or application. Users may change the configuration of the system as far as this is offered. Note that term **end-user** is also sometimes utilised with the same meaning. Users may have different roles, e.g. being a customer – then the user is a data subject – or being an employee of the data controller or the data processor – then the user is also a data subject in the sense that the employer is processing the employee's personal data; an employee working with personal data of customers according to the rules of the organisation is representing this organisation (i.e. the data controller or the data processor).

The aforementioned terminology and roles are followed in the descriptions within the rest of the document.

2.3.4 Relationship between data protection by design and data protection by default

As already mentioned earlier, data protection by design and by default and closely related.

For instance, an implementation of data protection by design (as well as of security of processing) could be that an IT system automatically encrypts any data transfer without the need or the possibility of users to change that functionality. In this case, the encryption functionality is wired-in. This also contributes to the principle of data protection by default, since encryption limits the accessibility of the personal data[9].

In addition, data protection by default is specifically relevant whenever the setting can be changed, e.g. by choice of the user. In this case, the default setting has to be configured in a way that minimises data and data processing, thereby also limiting the possible risks, taking into account the purpose of the processing. For example, in many mobile apps location data are not necessary for the purpose of the app, yet they are often collected by default [Chitkara, 2017]. A data-protection-friendly default setting in such a case would be to refrain from accessing or processing in any other way the mobile phone's location data.

Depending on the purpose, however, default settings for the processing of the same type of data might be different if for instance these data are necessary for the specific data processing operation. For example, some apps provide location-based information, e.g. for sending vouchers for a café nearby or for navigating the user to the nearest pharmacy and, thus, require access to the mobile's phone location data (otherwise the service cannot be offered). If this is the purpose of the app and the users have been informed about it (e.g. through a dedicated pop-up message during the first time it was executed), the default setting would probably reasonably include the access to location data.

The possibility to change the defaults is also equally important to this end. For example, a user of an app that initially does not access location data may decide in a conscious choice to disclose this information later for the additional purpose of getting location-based information [Datatilsynet, 2018]. In this case, the user may actively choose to change the pre-configured data-protection-friendly settings, thus making the location data available to the app[10]. Similarly, the user may choose to deactivate the collection of location data, thus reverting to the data-protection-friendly default. In both cases, it is important that the user can change his/her choices easily and without being prejudiced towards specific ones. Moreover, since the default setting has to reflect the necessary data processing regarding the purpose, a change should not be

[9] This of course is also clearly related to the encryption technique applied, as well as the parties that may have access to the underlying cryptographic keys.

[10] This change would act as a freely given, informed expression of the user's will – as demanded for valid consent (see Article 4(11) and Article 7 GDPR on consent). The requirement of being informed can be derived from the data-protection principle of transparency (Article 5(1)(a) GDPR).

required for realising at least the basic functionality. In other words, a change of the pre-setting should not be crucial for the functional capability of the data processing.

Although data protection by design and data protection by default seem to be like twins in their structure, sharing the same idea of building in data-protection functionality and thereby making it easier for data controllers to comply with the legal data-protection framework and for users to maintain their private sphere, the structure in Article 25 GDPR differs between the "by design" and the "by default" parts.

Article 25(1) GDPR is a refinement of Article 24(1) GDPR that states the responsibility of the data controller for processing the data according to the Regulation. Both Articles – as well as the security norm Article 32(1) GDPR – start with a prefix text on conditions that have to be taken into account when determining the appropriate technical and organisational measures. While Article 24(1) GDPR limits its perspective to the conditions of *"the nature, scope, context and purposes of processing"* on the one hand and on *"the risks of varying likelihood and severity for the rights and freedoms of natural persons"* on the other hand, both Article 25(1) and Article 32(1) GDPR extend their view on *"the state of the art"* and *"the cost of implementation"*. These conditions constitute the criteria that have to be balanced by the data controller as a basis for its decision on the technical and organisational measures.

The choice of measures to take and the waiver of other measures have to reflect the proportionality principle. Having said that, the character of Article 25(2) GDPR stands out as it is not formulated in a relative way (i.e. not beginning with *"taking into account"*), but the demand of the appropriate default setting is expressed in absolute terms – it stipulates a guarantee for protection with respect to data minimisation, at least in the beginning of the data processing [Bygrave 2017]. This is in line with the character of the GDPR since Article 25(2) GDPR mainly repeats the data-protection principles concerning necessity of personal data for a purpose, but applies it to the technical realisation. As a result, whenever default settings play a role, they must adhere to the requirements of necessity for the respective purposes.

2.4 Understanding data protection by default

2.4.1 Data controllers as addressee of data protection by default

The obligation for data protection by default in GDPR is directed only to the data controller. Unlike other demands of the Regulation, e.g. on implementing technical and organisational measures for security (cf. Article 32 GDPR), the data processor is not directly addressed by Article 25 GDPR.

Similarly, Article 25 GDPR does not directly target "producers of the products, services and applications"; these stakeholders are only mentioned in Recital 78, sentence 4: *"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."* The said encouragement could be accomplished by data controllers when determining the means for the processing, in particular when selecting the products, services and applications to be employed for the planned data processing. For instance, data protection by default (and by design) could be set as a requirement in any procurement process from the data controller as far as processing of personal data is concerned. In such cases, a minimum requirement from the data controller's perspective could be to demand from producers of products, services and applications that they facilitate the data controller to set the data-protection-friendly default before release (e.g. by evidently providing information on product's operations, pre-settings and available choices). Of course, it can be helpful if the producer directly applies the GDPR and therefore the appropriate data-protection-friendly defaults have already been pre-configured. By applying this requirement to the data controller's

process of procurement, selection and configuration, the GDPR will achieve an indirect effect on data processors or producers with regard to data protection by design and by default.

2.4.2 Effect on producers of products, services and applications

The indirect effect of data protection by default to producers of products, services and applications should not be underestimated. A data controller that seeks compliance with GDPR would probably not knowingly purchase products or enter into contacts with service providers as data processors where the obligation of data protection by default cannot be fulfilled.

However, the current market situation is characterised by deficiencies in widely used software and services. A recent report of the Norwegian Consumer Council even lists privacy-intrusive defaults of well-known services and application providers. [Forbrukerrådet, 2018]. Clearly, these companies are not only producers, but often act as data controllers themselves and are therefore directly subject to the requirements of the GDPR including data protection by default. This holds for many producers of products, services and applications who are not only software developers (with no relationship to any natural person as customer) but have contracts with their users. In these cases they process their users' personal data at the very least in the form of unique identifiers, e.g. for providing regular updates or analysis of usage patterns. Still, there are hardware and software developers with no own processing of personal data. Here, the organisation that employs that hardware or software is the data controller and thereby solely responsible for implementing the data-protection-friendly defaults whenever processing of personal data is affected, e.g. personal data of customers or of employees. It is important that the defaults are properly implemented before the role-out and the beginning of the data processing.

It is interesting to note that, while the GDPR refrains from directly placing producers under an obligation but only relies on an indirect effect on the market, the proposal of the ePrivacy Regulation from the European Commission takes a different approach, as it contains demands on functionality of the software [European Commission, 2017][11]. However, the ePrivacy Regulation is not in force yet and the concept of requirements which address the software used for communication may not be retained in the final text[12].

2.4.3 General decisions in the design process

In the design process of IT systems or IT-based services, the producer of such a system or service, needs to take the decision whether some specific functionality or behaviour of the system or service is being built in or is rather configurable, as shown in Fig. 1. For each configurable part, it has then to be decided whether there is a pre-setting or not (i.e.: no default selection; the user would be forced to explicitly choose the setting before use). For each pre-setting, the configuration that fulfils Article 25(2) GDPR has to be determined and implemented. This can be done by the producer or the data controller, on the basis of the information provided by the producer, who deploys the relevant system or service for a specific data processing operation (see also section 2.4.1). In any case, the data controller is the one responsible under GDPR for data protection by default and, thus, needs to able to understand the default settings in the system or service, as well as the possible choices for changing the defaults.

---

[11] In particular, Article (10) of the EC proposal demands that "*Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment*". The same article also provides that "*Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting*".

[12] On 19 October 2018, the Council of the European Union presented a revised version of the Proposal for an ePrivacy Regulation that omits Article 10, https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/91/EU_39172/imfname_10848802.pdf. This, among others, will be subject of further discussions among the European Commission, the Council and the Parliament.

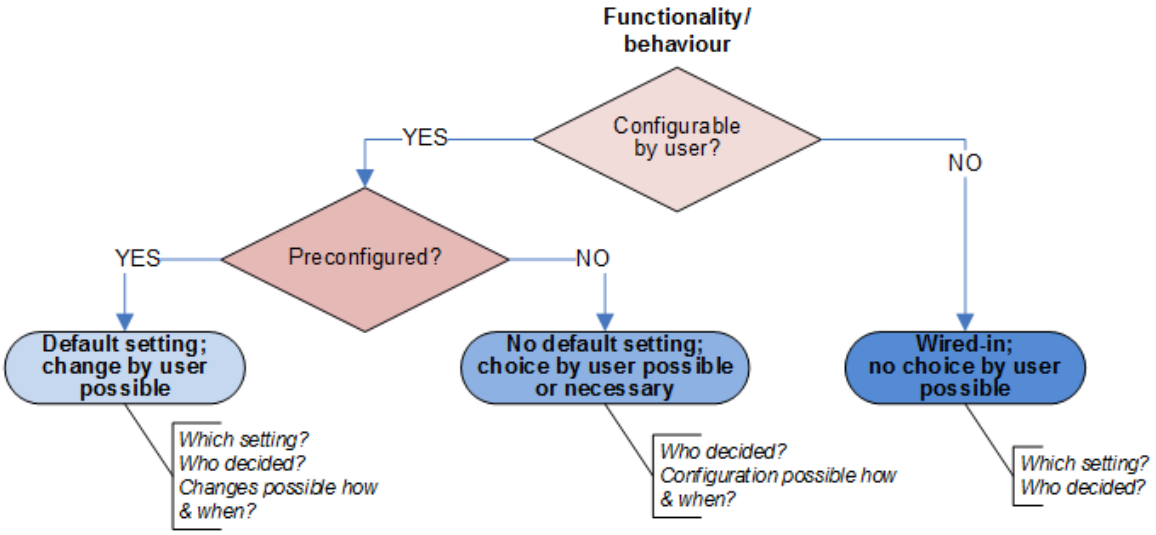

Fig. 1: Overview on choices in the design process regarding functionality or behaviour of an IT system (on the basis of [Bieker, 2017])

The data protection by default principle does not necessarily imply that a pre-configured default is reasonable in all situations. For instance, other legal obligations may prevent specific pre-settings or prohibit defaults at all because an explicit decision by the user is regarded as mandatory, e.g. on the basis of consumer protection law. Still, a meaningful default setting in the sense of Article 25(2) GDPR would in many cases be preferable (from a data protection point of view) over putting the burden on the users for each single configuration option.

2.4.4 Criteria for setting the defaults

As already highlighted, the data controller is the responsible actor for the default setting. It has to implement the 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. For instance, this could be a limitation of what is being disclosed on the end-user's side. On the other hand, it could also be a limitation of what is being analysed or otherwise processed on the data controller's side. As an example, in the case of an Internet browser[13] that is installed at the user's side without any further data processing, the browser's manufacturer would not be a data controller with the responsibility over user data, but only a software producer that is not addressed by the GDPR. The browser could be configured in a way that omits disclosure of some usage information, but due to technical reasons data such as the IP address, the screen resolution or the browser version – the entire, often identifying browser fingerprint[14] – would probably be transmitted when the user visits an online service offered by a data controller. In such case, a good practice for the data controller would be to refrain by default from analysing the disclosed information, as long as this is not necessary for a specific data processing purpose.[15]

[13] Note that the ePrivacy Regulation that defines requirements for software such as Internet browsers is not effective, yet. In the meantime, data protection legislation that has been put into force including the GDPR applies to all processing of personal data.
[14] See also: Article 29 Data Protection Working Party opinion on device fingerprinting [WP29, 2014b].
[15] However, the browser manufacturers could support this behaviour by communicating that tracking of the user's behaviour is not desired unless explicitly stated otherwise. Note that the communication of the user's expressed preference concerning being tracked is subject of the W3C Candidate Recommendation on "Tracking Preference Expression (DNT)". Since the W3C specification does not aim at substituting "regulatory, legal, or other regional requirements regarding tracking" (including the GDPR), does not

To this end, concerning the "data protection by default" requirement, reference is made to the principles of purpose binding, data minimisation and storage limitation. They are reflected by four criteria in Article 25(2) GDPR that characterise a data-protection-friendly default and should, thus, be used by controllers when defining the defaults:

- **Criterion 1: Minimum amount of personal data**

  The amount of personal data has to be the minimum for the purpose. This does not mean that the number of bits is reduced as much as possible; instead, the alternatives of data sets whose collection could be less infringing concerning the private sphere of an individual have to be compared with each other. It could be fewer attributes, of less sensitive data. Obviously the amount of personal data can be decreased, too, if the data are not, or less, personally identifiable. This could be aggregated information that yields anonymous data or it could also be pseudonymised data where the additional information is kept without access of others.

- **Criterion 2: Minimum extent of the processing of personal data**

  The personal data processing should also be minimised according to each specific purpose, e.g. limitation of whether data are stored at all, whether and how the data are analysed once or multiple times, whether the data are transferred to other recipients, whether the data are linked with other information, e.g. for profiling purposes (Article 21 GDPR). In this regard, the provision of effective tools (by the controller) that can facilitate the exercise of data subjects' rights is also very strongly linked to minimising the extent of the processing, while contributing to the overall empowerment of the data subjects' to this end.

- **Criterion 3: Minimum period of the storage of the personal data**

  Clearly, the period of storage of personal data by the controller plays an important role. With respect to the purpose, the minimum time for storing the personal data has to be chosen. This could mean no storage at all, or an anonymisation or erasure as soon as possible.

- **Criterion 4: Minimum accessibility of the personal data**

  Accessibility in Article 25(2) GDPR tackles possible access by any entity (people such as other users, organisations such as the data controller or government authorities, machines such as search engines or cloud servers). The accessibility depends on where the data are stored or processed, how the access is limited by assigned access rights, whether the data is stored or processed in clear text or in an encrypted matter and who could decrypt the data, who the recipients of the data are, and whether multiple copies, including not securely erased files, may exist that can be accessed by others. The location of storage and processing is important to determine the accessibility, e.g. the difference between a local processing on a device on the user's side and the central processing in a cloud or on servers on the data controller's side. Limiting the accessibility also means to limit the storage in jurisdictions where the law allows governmental access without sufficient guarantees for the

demand for a preconfigured "no tracking" by default [Fielding, 2017, section 10.1]. Instead, the W3C specification points to whether "the recipients believe that the signal has been deliberately and knowingly configured".

protection of personal data. Also, when emitting personal data the range should be narrowed as far as possible concerning the purpose to prevent unauthorised accessibility.[16]

With regard to accessibility, it is interesting to note that Article 25(2) GDPR specifies that by default that personal data must not be made accessible without the individual's intervention to an indefinite number of natural persons. As a consequence, the data controller should implement technical and organisational measures that prevent personal data from being made public by default [EDPS, 2018, p. 12]. This provision can be especially relevant in the case of social networks [Hansen, 2013] or for data sharing in an Internet-of-things scenario [Article 29, 2014, p. 23] or for data exposure via search engines [IWGDPT, 2013].

2.4.5 Assessing and documenting the defaults

Before the processing starts, the purpose and the necessary data have to be specified [ICO 2018]. Taking into consideration the four criteria mentioned in 2.4.5, a starting point for data controllers could be to list all purposes of the processing operations, and assess and document for each specific purpose if the chosen defaults are data-protection-friendly. This process can support data controllers selecting the appropriate defaults and eventually could constitute the basis for compliance with Article 25(2) GDPR. It may be obvious which data items have to be processed to achieve a specific purpose. However, often there is the potential for minimising the set of data, e.g. if the real name is not necessary, but a pseudonym would suffice; e.g. if the exact birthdate is not necessary, but only proof for being of age; if the device ID is needed for the technical interaction, but no longer than a session and thus changing identifiers with limited validity would have to be preferred. The same holds for the minimum extent of data processing, minimum storage period and minimum accessibility.

Striving for the data-protection-friendly defaults, can also help the data controller look for other options that may present a means of a less infringing measure. This requirement is not newly generated by Article 25 GDPR, but has to be fulfilled anyhow according to the data-protection principles of necessity, data minimisation and storage limitation laid down in Article 5 GDPR. Though, Article 25 GDPR sets a focus on designing the data processing where not only the data categories play a role, but technical solutions for limiting the data processing to the utmost extent have to be taken into consideration. This approach encompasses also those data items that only are being used for technical purposes, e.g. temporary files or additional data that, solely or in combination, may be identifying information, such as the browser fingerprint. Further, for evaluating the accessibility of the data, the data controller will have to check possible accesses from service providers or other parties. This means that putting the data processing into a cloud, the accessibility check would have to consider also the cloud provider as well as governmental authorities that may enforce the access to those data.

Furthermore, Recital 78 of the GDPR points out that *"[i]n order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default"*. It is a good practice that such internal policies are documented in written form; typically, these inner-organisational directives are enacted by management and communicated to all employees. Those internal policies may contain information on how Article 25 GDPR is implemented in the organisation, e.g. how it is ensured that the GDPR requirements will be considered *"both at the time of the determination of the means for processing and at the time of the processing itself"*, as demanded by Article 25(1) GDPR. This calls for building a culture of awareness for data protection within the organisation, with senior management and data

[16] This is for instance covered by the following recommendation concerning connected vehicles: "Standards for the implementation of the Cooperative Intelligent Transportation Systems (C-ITS) should limit the diffusion of information only to vehicles and infrastructure entities within close range of the emitting vehicle." [IWGDPT, 2018, p. 12].

protection teams as good examples. It should become a core property woven into all organisation policies and procedures.

With respect to the defaults of processing, the responsibilities concerning the decision on the exact setting and its regular evaluation whether it is still an appropriate default have to be determined. Also, data protection by default should be – as well as data protection by design – a requirement that is to be made explicit as an essential factor in any development, design or procurement endeavour. Before releasing a new system or new process, the compliance with data protection by design and by default should be tested and checked; also appropriate defaults should be specified.

2.4.6 Additional issues for the data controller concerning the default

The principle of data protection by default complements other data protection requirements in the GDPR. For instance, "security by default" – not phrased that way, but could be derived from the security requirements laid down in Article 32 GDPR – can be regarded as an implementation of both data protection by default and by data protection by design that, by definition in Article 25(1) GDPR, demands building in all data-protection principles including security (Article 5(1)f GDPR) – see also Section 2.5.

Of high importance is the data-protection principle of transparency (Article 5(1)a GDPR), being substantiated in Articles 13 and 14 GDPR: the data controller is obligated to provide information about the data processing and the data subject rights to the data subjects, whereby this has to be realised *"in a concise, transparent, intelligible and easily accessible form, using clear and plain language"* (Article 12(1) GDPR). To this end, if the starting point is a data-protection-friendly pre-setting, it is essential that the user is informed not only about the properties of the current configuration, but also the possible effects of changing the pre-setting. This encompasses, among other, if additional purposes of data processing will be pursued, if further recipients may get access to the data, if the data may be stored for a longer time, etc. If the data processing is being modified, e.g. when products or services are updated, this would also require that the data controller informs the data subject accordingly. If an update demands a new default setting, this specifically should be explained (since the user would not expect this). However, overriding a configuration that a user has diligently elaborated should only happen under exceptional circumstances, e.g. if it is necessary to mitigate a risk. Again, transparency about the changes and the reason for that is important.

The principle of fairness should also be governing the determination of the purpose of the data processing: It is important that data controllers consider a basic functionality that can easily constitute a data minimising default – aiming at minimising the risk for the rights and freedoms of natural persons [Hansen, 2018], instead of constructing a largely sophisticated purpose and overloading it with supposedly needed functionality or otherwise using "dark patterns" in system design [Forbrukerrådet, 2018]. This would not only help implement the principle of data protection by default of the GDPR, but provide a way to gain the users' trust in the data controller. Indeed, if the users have the justified feeling that they are treated with respect and fairness, it seems more likely that they will give informed and free consent for further data processing. What is more, users can collect experiences on the basis of simple usage possibilities and learn to estimate and handle potential risks before being exposed to a scenario that is too complex and overwhelming for inexperienced users.

The same spirit calls for user options that do not throw all data protection guarantees over board once the first change is made [Hansen, 2017, p. 35], but enable gradual modifications, e.g. in the extent of data processing [ENISA, 2017, p. 51]. If further purposes are introduced, these will shape the new default. If the purpose is characterised by further sharing of information (e.g. with friends in a social network) as far as the user agrees to, the purpose as such would not change, but the user will tailor the amount of disclosure or processing according to the specific scenario. The preference of gradual changes does not exclude

meaningful clustering, e.g. that users would not have to specify for each friend which data items to share, but could group the acquaintances and define per-group settings for determining what to share.

This illustrates an ambiguous relation between data protection by default and usability requirements. On the one hand, basic settings and purposes as well as the related risk are much easier to understand and to control. This can support usability. On the other hand, the configured default may in certain cases restrict the functionality, e.g. if as a default the data controller keeps less data about a user, if the system does not demand user accounts that provide configuration possibilities valid for future use, if processing in the cloud is minimised and therefore the usage across different devices is less supported, or if the system dispenses with personalisation, thereby potentially sacrificing some usage convenience. All these examples can be countered by clever design strategies, e.g. by additional tools on the user side that facilitate communicating additional information only if and when desired by the user. Also, users may give consent for personalised services after being informed about the data processing and the consequences. Still, this does not go against a data-protection-friendly default as a starting point.

In a world of widely distributed "dark patterns" that nudge users into privacy-adverse behaviour, as a countermovement thought should be given to design patterns and defaults that may urge users towards privacy-friendly choices. However, this must not be misunderstood as a manipulation of people: The "good purpose" of better data protection does not justify the means. Therefore, transparency and fairness are of utmost importance.

2.5 Security by default

Similarly to the concept of data protection by default, which aims at putting data protection first, *security by default* refers to *putting security first*, or otherwise, making security the key element of the initial configuration of products, services or applications. One could argue that these two concepts are actually very closely linked (a comparison to the notions of security by design and privacy by design is also relevant to this end). Indeed, if the preconfigured settings are by default adhering to a high level of security protection, it is reasonable to expect that personal data will also be subject to a high protection level. On the other way round, as security is a fundamental principle of data protection, privacy-friendly settings will also preserve by default the security of personal data.

Still, having said that, there are certain differences between the two. Data protection defaults seek to address the requirements regarding the protection of personal data, which are not only security-related. On the other hand, security defaults refer to all types of products, systems and services (and not only those processing personal data). Moreover, despite their interconnection, there might also be cases of tension between security defaults and personal data protection principles (e.g. in cases where the security defaults might lead to increased monitoring or surveillance of data subjects). A balance between security and privacy requirements is, thus, necessary when the selection of the 'best possible' default is under consideration.

By the same token, GDPR provides (as discussed above and followed in the next Chapters) a specific framework for the determination of data protection defaults. Although this framework is generic enough, it still provides a good basis to start working on the 'correct' defaults. On the other hand, the notion of security defaults is not prescribed in a unified way, which leads to the discussion of what can actually be considered as secure default in certain cases. This is also quite relevant to defining the overall level of security of a product, service and application, in correlation with its purpose and user base. Usability aspects clearly also affect the adoption of security defaults, as well as technical and policy aspects (as for example in relevant discussions around encryption by default).

Due to the aforementioned reasons, the present document does not specifically deal with secure defaults. Still, we see the analysis of data protection defaults as a first step towards the analysis of security defaults, which is a matter relevant to all products, services and applications (including or not personal data).

3. Data protection by default in practice

This Chapter discusses the selection of privacy friendly defaults with the use of best practices and relevant examples, according to the criteria listed in Article 25(2) GDPR (see Chapter 2, section 2.4.5). Although each criterion is separately considered, they usually cannot be treated apart from each other. Instead, all criteria should be taken into account in a holistic approach. Furthermore, the measures for data protection by design and for data protection by default are overlapping, especially when it comes to data minimisation and storage minimisation. For instance, if specific privacy-enhancing technologies are employed that prevent the processing of the original personal data and use instead pseudonymised or anonymised data, this affects the degree of possible minimisation of personal data or their processing. Similarly, the adoption of security measures appropriate to the risk presented can also greatly influence the adoption of defaults. Thus, the best default would depend on how far security measures and data protection by design are implemented.

3.1 Best practices on data protection by default

In the next paragraphs, we refer to certain best practices for setting the defaults and illustrate indicative examples for each of the four criteria mentioned in section 2.4.5, i.e: minimum amount of personal data, minimum extent of the processing of personal data, minimum period of storage of personal data, minimum accessibility of personal data.

It should be pointed out that these examples aim to simply demonstrate how data protection by default can be applied in practice and the challenges that are inherent to this implementation; by no means should they be interpreted as a legal opinion on the corresponding cases.

3.1.1 Criterion 1: Minimum amount of personal data

Some best practices that the controller may have in mind, so as to minimise the amount of personal data collected and further used, are as follows:

- **The less data, the better**

  This is clearly the most obvious practice with regard to data minimisation, which also adheres to the well-known security 'need-to-know' principle. A simple case to demonstrate this is when the collection of personal data is done directly from the data subject, e.g. if a user is being asked to fill in personal data in an online form. Here, a data protection friendly default would start by minimising the amount of personal data that are collected. In particular, only those fields whose values are necessary for the specific purpose should be mandatory. In addition, if only standardised data values are asked for, a good practice would be to have them chosen from a list instead of offering a free text field where the user may fill in further unnecessary personal data. Having said that, it should be stressed that data minimisation does not only refer to minimising the data fields per se, but also to any other way of reducing data collection and further processing of data (following not only a quantitate but also a qualitative approach). To this end, minimisation may be achieved also by aggregating, counting, randomizing or anonymizing personal data, based on a privacy engineering approach (see also point made below on the use of privacy enhancing technologies).

- **Granular collection of data on the basis of necessity**

In some cases, multiple sub-purposes govern different phases of the processing. It is a good practice that defaults follow this granularity as well. For example, in an e-commerce scenario a user browsing the online shop would first decide on which items to purchase and only later would be asked for the name and the delivery address. Sometimes, a (not so data-protection-friendly) form may require filling in a phone number or the date of birth, although this information usually is not necessary for the purpose. While a phone number might be a practical add-on to call in case of problems with the delivery, the date of birth may be necessary for some payment methods – but only if the user chooses one of them. For instance, advance payment would not need an extensive data collection from the user. Such an approach may also be applied to more complex cases.

- **Use of privacy enhancing technologies**

  Data minimisation can in several instances be achieved by the use of security and privacy enhancing technologies, such as for example pseudonymisation or encryption techniques. Using the previous e-commerce scenario, it is often argued that the date of birth would be necessary in case of age restrictions for purchasing some goods, e.g. alcohol. Note that in this case the information for being of age does not require the exact date of birth, and not even the year of birth: Mechanisms such as privacy-enhancing attribute based credentials[17] or similar functionality on an ID card[18] can check whether the condition "being of age" is fulfilled and transfer only the result instead of the exact date of birth. Cryptographic techniques based on zero knowledge proof (ZKP)[19] can also be relevant in this regard. There is a multitude of privacy enhancing technologies today that can be used to minimize data collection and/or reduce identifiability of users [ENISA 2014], [ENISA 2015].

- **Different minimum per purpose**

  As already stated in Chapter 2, depending on the purpose, the 'minimum amount' differs for the same type of data. Therefore, the best practice for the controller is to re-assess defaults in all cases, following the specific data processing context.

  For example, in the area of mobile **apps**, location data is necessary only for specific purposes (and not all cases). Similarly, using the smartphone's microphone cannot be a general default although in some cases this might be needed. For instance, a karaoke game that evaluates the voice needs access to a microphone, but a camera app should not have access by default. Access to the address book of the smartphone and reading out other users' phone numbers would not constitute a proper default either: these persons may agree to have their numbers stored, but probably most of them would not agree to access by additional parties such as a service provider. Even some presumably negligible access rights of an app, e.g. to the battery status, may turn out to have sensitive impact [Olejnik, 2016] and thereby should not be processed by default.

  As another example, for **messengers** – and similarly for e-mail clients –, it should be considered how to minimise what – in addition to the message transfer between sender and recipient – is communicated to the other users by default: the log-in status, the read status of a message, the information that the

[17] Credentials that are based on attributes that users have in their possession.
[18] E.g. the German eID card. These mechanisms can also reduce the linkability by refraining from re-using the identifier for different purposes or with respect to various communication partners. This can contribute to a great extent to minimising personal data.
[19] A method by which an entity may prove to another entity that it knows a certain value X without disclosing any other further information between the two entities apart from the fact that X is known.

communication partner is in the process of writing a message etc. The data-protection-friendly configuration would start with the minimum extent of this information, but the users may decide to disclose more to their contacts. For the purpose "delivering a message" the default could be that the IT system informs the sender about the technical delivery status ("delivery in progress" / "delivered" / "not delivered because of <reasons>"), so that the sender can recognise if the recipient's address is not valid or if a technical problem prevents successful delivery. But the information whether the recipient has read the message would not be necessary for that purpose. A good practice to this end would be to ask the recipient whether he/she accepts that this information is sent to the sender (a practice which is actually embedded as a default in several email clients today).

- **Minimizing the risk**

  For determining the minimum amount of personal data, not only the size in bits and bytes is relevant. Instead, the objective is to minimise the risk with the effect that less sensitive data shall be preferred over sensitive data[20]. Similarly, anonymised data shall be preferred over pseudonymised data that again shall be preferred over non pseudonymised data (as long as strong anonymization or pseudonymisation techniques are applied). As an example, for video surveillance data, high-resolution face data combined with biometric analysis are more sensitive than low-resolution footage or blurred or blackened images of persons. Again, the use of security and privacy enhancing technologies can greatly support this goal.

- **Considering all copies and types of data**

  The requirement of minimising the amount of the personal data by default also encompasses reducing temporary copies or transfer of data as much as possible with respect to the purpose. Similarly, the potential generation of personal data in log entries should not be forgotten: If they are not necessary for the purpose, they should not be stored by default.

All the aforementioned practices can be used in combination with each other, as well as those practices mentioned under the next criteria.

3.1.2 Criterion 2: Minimum extent of the processing of the personal data

A key best practice that the controller can have in mind for this criterion is as follows:

- **The less processing, the better**

  Processing encompasses various possible kinds of operations or set of operations (see Article 4(1) GDPR). The requirement for 'minimum extent' does not mean to reduce the number of operations, but to minimise the risk for the rights and freedoms of natural persons. Thus, for example, it would mean to refrain from recording and storing the personal data if it is sufficient to do without it. For instance, processing the data only in the main memory instead of a storage device would be preferable if this is sufficient for the purpose. Usually this is rather a design decision and not so much a changeable default. However, it depicts the requirement for producers to think of ways to avoid permanent storage if there are purposes where this is not needed.

[20] See Article 9 GDPR on special categories of personal data, Article 10 GDPR on personal data relating to criminal convictions and offences or Article 87 GDPR on national identification numbers or any other identifier of general application.

As an example, for the purpose of **accessing websites**, the data-protection-friendly default would avoid the processing of personal data for user tracking or profiling. The processing of metadata (e.g. location data or camera data) embedded in a photo would not be necessary processing as a default for the purpose of **photo sharing**. Also, tagging people or biometric analysis of faces would not be necessary for this purpose and thereby should not be the default as this is the case in some social **networks**. For **smart meter** scenarios, the purpose usually does not require a transfer of energy consumption data to the providers every few seconds, but the intervals can be much larger, thereby minimising the extent of processing and reducing the risk to data subjects.[21] However, in all these cases, users may want to change the setting to enable other processing options for potentially extended purposes, e.g. personalised services.

- **User empowering tools**

  The limitation of the extent of the processing is closely interlinked with the provision by the controller of proper tools, which the data subjects can use to exercise their rights (Articles 12-20 GDPR). This includes data subjects' information, as well as an effective and easily accessible way (e.g. a dashboard) for the exercise of data subjects rights.

Clearly, 'less processing' includes also 'less data', 'less storage', as well as 'less accessibility'. Therefore, this criterion will in all cases be combined with many of the best practices mentioned in the rest of the Sections in this Chapter.

3.1.3 Criterion 3: Minimum period of the storage of the personal data

A key best practice that the controller can have in mind for this criterion is as follows:

- **Storage – the shorter, the better**

  For the personal data the storage period shall be minimised. Sometimes permanent storage is not necessary for the purpose at all, but often the purpose requires storage for some time after which the personal data have to be erased[22]. This extends not only to data in a data base, but also encompasses temporary copies or personal data in log entries where the storage time, or the time until the data expires and is (potentially automatically[23]) erased, is minimised.

  As an example, in the case that a data controller runs an **online user survey**, a good practice would be that, by default, the individual responses of the users are not locally stored in their computers (once the user has submitted his/her answers to the survey), so as to avoid linkage between the user and his/her responses. This would be especially important in cases where the users' identity does not need to be preserved and in particular, when the computer is utilised by several users. Of course, such as measure would also need to be complemented by other protection measures that would reduce the users' identifiability to the least possible extent. Note, however, that the default might be different in case of temporary storage of the user's responses (before final submission).

It should be noted that the minimisation of storage may also be based on the use of security and privacy enhancing technologies, as well as on the minimisation of the overall extent of the processing, as mentioned earlier.

---

[21] See also: Article 29 Working Party opinion on the Internet of Things [WP29, 2014a].
[22] "Erasure" means a secure deletion without any residue and no possibility to reconstruct the personal data.
[23] This, again, is a data protection by design functionality.

3.1.4 Criterion 4: Minimum accessibility of the personal data

Some best practices that the controller may have in mind, so as to minimise the amount of personal data collected and further used, are as follows:

- **Restricting access on the basis of necessity**

  The requirement of minimum accessibility is clearly relating to access policy and access control, which should designed by the controller on the basis of the need-to-know principle (which is also a basic security principle). This is achievable by separation of data per purpose, e.g. in different locations, servers or data bases. What is more, tailored access rights support this objective. It must not be forgotten, that the integration of service providers[24], such as cloud providers, means additional access possibilities for their employees. Also, there exists the risk of further access by governmental authorities, especially in remote clouds.

- **Limiting ways of sharing**

  Furthermore, the different possible ways of data sharing should be assessed and, wherever possible, minimised by the controller. The accessibility grows if personal data are copied, transferred to other recipients, made available to selected friends, published or provided to search engine crawlers or other machines that may process the personal data.

- **No public by default without active intervention**

  Article 25(2) GDPR contains a specific requirement on providing accessibility of the personal data for an indefinite number of natural persons only after the individual's intervention. This aims at preventing personal data from being made public by default; publishing personal data would need a conscious act on the basis of sufficient information about the data processing.

  As an example, for **social networks** a best practice could be to limit automatic accessibility of personal data to oneself and possibly a small circle of friends. A wider circle could quickly grow into an "indefinite number of natural persons", e.g. by transferring data to friends-of-friends, making the data public, or providing accessibility by global Internet search engines. A data-protection-friendly default would avoid all of this, whilst still allowing the user to explicitly choose wider accessibility settings. Following this logic, for instance, an **announcement of a private festivity** on a social network should not be automatically visible to the public.[25] Similarly, Internet search engines (that will use the content for indexing it and showing hits to search requests publicly) should -by default- refrain from accessing the social network data items. A related scenario is the uploading of self-measuring of health values or **fitness tracker** patterns that may reveal personal data to others: a best practice for the controller would be that -by default- these data are not shared with other users or made otherwise accessible unless the user explicitly authorises this. Moreover, with regard to personal data exposure through **search engines**, as a general good practice, controllers should take into account mechanisms that limit the indexability of websites[26] (and, thus, further publication of personal data).

[24] Note that service providers may legally act on behalf of the data controller, namely as data processor.
[25] Y. Wang et al.: "I regretted the minute I pressed share": A Qualitative Study of Regrets on Facebook, in: Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11), pp. 10:1--10:16.
[26] For example the use of robots.txt or the metatag noindex, see also in [IWGDPT, 2013].

Again, all the aforementioned practices should be combined with practices discussed under other criteria, as well as broader data protection by design methodologies that the controller might be following.

3.2 Defaults and usability

As mentioned earlier, defaults are an important parameter for enhancing usability in systems and applications by allowing simple use, i.e. refraining from asking users to make multiple choices (which would hinder the overall functionality). In this way, defaults can contribute towards user-friendly systems, supporting the user's tasks and in general providing a satisfying user experience.

However, in order for defaults to be a parameter of usability, it is of utmost importance that they do not 'hide' certain aspects of functionality from the users or, even worse, urge users towards functionality that would not be in principle desirable or expected. Unfortunately, as already discussed, this is not always the case in the area of privacy and data protection. On the contrary, it is quite common that specific design patterns aim at directing users towards non-privacy friendly choices, often with the promise or presentation of a better interface ("look and feel"). This phenomenon is not at all new; in a multitude of online services, it is hard for users to exercise their rights or even to find adequate information about the personal data processing in the first place.

The GDPR in Article 25 aims to tackle the aforementioned issues, while supporting usability, since –if privacy protection settings are already in place- the need for asking users to make privacy choices (e.g. by means of repetitive banners or pop-up windows) will be significantly reduced. Still, there are some additional dimensions that need to be considered by the controller with regard to usability, especially when putting defaults into practice.

First of all, it has been shown that, even if the defaults are privacy-aware, the interplay with other components and services is also essential (and might actually require the change of these defaults) [Leon, 2012]. To this end, it is important to pay attention that a change of pre-configured defaults settings is done with appropriate granularity, thereby ensuring that users' protection is not fully 'lost' at once [ENISA 2017]. Moreover, after having changed the pre-configured "data protection by default" setting, users should be able to easily go back to this default setting.

In addition, attention should be paid so that the 'data protection defaults' are not such that the system or application becomes difficult (or even impossible for the average user to use) and, thus, a change of the defaults is immediately needed. This is a situation that often occurs in practice, where the 'privacy option' is far more complex than the alternative; defaults, however, should not be designed in such an impactful way for both usability and data protection. In fact, privacy friendly defaults should actually refer to *reasonable* defaults, in the sense that they should adhere to the users' expectations with regard to the processing of their data. This is also quite relevant for security defaults (see Section 2.5). In defining reasonable defaults, the target user groups are also essential to consider, e.g. different settings might be needed for children and adults, or different settings for EU residents and non-EU residents when it comes to storage location [Hansen, 2017].

To this end, a static 'take it or leave it' default that highly restricts functionally is not an acceptable approach. Instead, defaults should be adopted on the basis of the purpose of the processing following a granular approach, where additional (but limited) user configuration could be required depending on the case. Indeed, taking the pre-configured default as a starting point, users should be supported in choosing the best fitting configuration (see e.g. [Ravichandran, 2009]), or they could even profit from the approach of "on the fly" privacy management for adapting and organising their own privacy preferences [Angulo, 2012]. The interplay between data protection and security defaults is also an essential parameter to this end (see also Section 2.5).

Following the aforementioned discussion, determining the 'correct' defaults is in fact a direct matter of usability (as well as of data protection). As such, it has to be performed with caution, as, once defined, defaults create a norm, which is often very difficult to change [Kesan, 2006].

4. Data protection by default guiding questions

The data controllers' obligation to comply with GDPR is obviously not limited to one specific article or paragraph in the Regulation. However, to understand the gist of the new requirement of data protection by default, in this Chapter we present a list of relevant questions that a data controller could use for a self-check. This list should only be considered as guidance towards assessing the defaults and is not exhaustive. Note that not all requirements apply equally to all organisations, or to all possible purposes of data processing.

In addition, these self-assessment questions may also be useful for producers of products, services and applications to appropriately integrate data protection by design and by default in their production procedure(s) and (eventually) support data controllers. For instance, by providing the necessary documentation, deciding how to build in data protection requirements and choosing the most appropriate and risk-minimising default setting, the producers may provide a solid starting point to controllers who opt for those producer' products, services or applications. Designing security by default options could also benefit from such an approach.

4.1 Guiding questions for understanding the data processing operations

An essential prerequisite for all compliance analyses – and thereby for accountability – is that the data controller has a good understanding and knowledge of the scope and the function(s) of the personal data processing operation.

Therefore, also with regard to the defaults, the starting point is the determination of the purposes of processing. Following the discussions in Chapters 2 and 3, for each specific purpose the following criteria can be set:

- Criterion 1: Minimum amount of personal data
- Criterion 2: Minimum extent of the processing of the personal data
- Criterion 3: Minimum period of the storage of the personal data
- Criterion 4: Minimum accessibility of the personal data

For each one of these criteria a list of non-exhaustive guiding self-assessment questions that can be relevant also for the selecting the defaults is presented below.

4.1.1 Criterion 1: Minimum amount of personal data

The data controller can consider the following key aspects with regard to minimising the amount of personal data:

- Are all personal data items necessary for the specific purpose of the processing? Can this necessity be justified?

- Could the purpose be achieved with fewer or less sensitive[27] data items?
  Should this is the case, the controller should seek to define the set of data items that could qualify as a minimum and justify why this minimum data set is not preferred (to the chosen data set).

[27] "Less sensitive" could mean e.g. to skip data as characterised in Articles 9 and 10 GDPR, to restrict the linkability and therefore refrain from identifiers of general application or to have aggregated or blurred or fully anonymised data.

- Are there any temporary copies of personal data items created?
  Should this is the case, the controller should seek to justify why these copies are necessary for the specific purpose.

- Are there any log entries related to the processing created? Do they include personal data?
  Should this is the case, the controller should seek to justify why the logs are necessary for the specific purpose.

Overall, the scope of the questions under criterion 1 is to help the controller rethink the data that are being used and reassess if in all cases their processing is needed. This exercise is clearly related also to the overall extent of the processing (see next Section).

4.1.2 Criterion 2: Minimum extent of the processing of the personal data

The data controller can consider the following key aspects with regard to minimising the extent of the overall processing of personal data:

- Are all types of processing operations of the personal data necessary for the purpose[28]? Can their necessity be justified?

- For each processing of the personal data, is it ensured that there is no possibility for substituting it by another way (less intrusive) of processing (e.g. instead of storing data only processing it in the main memory)? Can this be justified?
  In case where there are other alternative (less intrusive) ways of processing, the controller should reconsider the approach used, or otherwise justify why the chosen approach is still preferred over the alternative.

- Does the processing include automated decision-making, including profiling? Is this necessary for the purpose of the processing?
  Should this is the case, the controller should explain in more detail the overall context of this processing (e.g. types of personal data, purpose, processing means, safeguards).

- Does the processing include any transfer of personal data to other recipients, specifically to a third country? Can this be justified for the specific purpose?
  Should this is the case, the controller should explain the specific conditions (e.g. types of personal data, specific recipients, purpose, relevant safeguards).

- Does the processing include any processing of sensitive data? Can this be justified for the specific purpose?
  Should this is the case, the controller should explain in more detail the specific context (e.g. types of personal data, purpose, relevant safeguards).

Overall, the scope under this criterion is that the controller explains and reassesses in more detail how the minimum extent of processing of personal data is implemented by specific processing operations.

[28] Note that processing of temporary copies and of log entries also has to be considered here.

4.1.3 Criterion 3: Minimum period of the storage of the personal data

The data controller can consider the following key aspects with regard to minimising the storage of personal data:

- Does any storage of personal data take place in the context of the specific processing operation?
- Should this is the case, what is the storage period that is necessary for the purpose? Can it be justified in relation to the purpose of the processing?
- Does the storage period vary between different data items?
  In such cases, the controller should try to define (and justify) specific storage periods for different data items.
- Are data erased after the end of their defined storage period?
  If this is not the case, the controller should explain the purpose for which the data are further processed, how storage is performed (location, recipient) and the planned retention period.

Overall, the scope of this criterion is to put the data controller into the logic of miminising retention periods in all cases when storage is no or no longer needed for a specific data processing operation.

4.1.4 Criterion 4: Minimum accessibility of the personal data

The data controller can consider the following key aspects with regard to minimising accessibility to the personal data:

- Has the accessibility of each personal data item (access rights) been defined? Can its necessity be justified for the specific purpose?
- Has the location of processing been chosen to minimise accessibility as far as possible for the purpose (e.g. separated from data processed for other purposes, preferring local storage over remote storage)?
- Are the access rights to the personal data limited according to the need-to-know principle as necessary for the purpose and by what means?
  Should this is not the case, the controller should seek to justify further access possibilities.
- Have any security and privacy enhancing technologies been applied (e.g. encryption or pseudonymisation), so as to limit access to the minimum extent, and by what means?
- In addition to what is necessary for the purpose, can it be ensured that there are no further recipients or copies or log entries that may be personal data (with further accessibility) and by what means?
  Should this is not the case, the controller should provide relevant justification.
- When the personal data are erased, can it be ensured that no traces are left so that the personal data cannot be reconstructed? This also holds for data at recipients, temporary copies or log entries with respect to the necessity for the purpose.
  Should this not the case, the controller should be able to provide relevant justifications.
- For each personal data item, it there any public or far-reaching accessibility, i.e. accessibility to an indefinite number of natural persons?

Should this is the case, the controller should be able to define for which personal data items and under which conditions. Moreover, if public or far-reaching accessibility is possible albeit not the default, the controller should explain the interactions that are necessary for this far-reaching accessibility. The controller should also assess if adequate information has been provided to the individuals (Articles 13 and 14 GDPR).

It should be pointed out that most of questions presented in Sections 4.1.1 to 4.1.2 are in fact important design questions that need to be considered at the moment where the requirements for the IT system or service are set. Still, they are also integral for defining the defaults, in combination with the specific questions addressed in section 4.2.

4.2 Guiding questions for defining the defaults

The following list of questions aims at supporting the controller, as well as the producer of products, services and applications to define data protection friendly defaults. Having said that, it is important to note that, depending on the case, some questions might be more relevant to controllers and others to producers.

The questions are presented having in mind that for each new IT system or IT-based service, the producer needs to define: a) which functionality is built into the system without the possibility of change, and b) which functionality is configurable by the user, i.e. the end-user or the data controller before releasing it to other users. For the configurable functionality the producer has to decide whether the configuration is left to the user or otherwise determined in a default pre-setting.

Moreover, the producer or the data controller that employs the system needs to select the appropriate data protection friendly defaults. In any case, the data controller needs to be able to understand the defaults, as well as the options for changing them (on the basis of relevant information provided by the producer).

To this end, the following questions can support the decision process:

- What are the specific purposes of the data processing? Are the data subjects informed about the purposes and the data processing[29]?

- For any built-in functionality:
  - Are there situations conceivable where users would prefer or need a different functionality? In which way?
  - Does the built-in functionality implement the data protection principles of the GDPR? Which data-protection principles are supported by this functionality, which are not?

- For any configuration option:
  - Which are the possible settings/options?
  - Which are the settings/options that minimise the amount of personal data, the extent of processing, the storage period and the accessibility taking into account each specific purpose? Is this the default pre-setting? (see also Section 4.1)
  - If more than one setting may come into question, are there specific criteria for preferring one setting? (This could be the case for different target groups, e.g. different pre-settings for children.)
  - How are the alternative choices presented so that the user can make a privacy-aware decision?

[29] As well as providing the other necessary information as laid down in Articles 13 and 14 GDPR.

- For any configuration option without a default pre-setting: What is the reason for not using a pre-setting?

- For any configuration option with a default pre-setting:
  - Does the default setting realise that only personal data which are necessary for each specific purpose of the processing are processed? (see section 4.1).With respect to:
    - the amount of personal data collected (can there be less personal data, e.g. fewer attributes, aggregated information, less sensitive data, no (temporary) copies?),
    - the extent of their processing (can the processing be reduced, e.g. less analysis, less transfer, less linkage with other data?),
    - the period of their storage (can the storage period be shortened?) and
    - their accessibility (can the amount of people or parties or machines that will or may have access to the personal data can be decreased, e.g. by local storage, limited access rights, encryption, secure erasure without any traces?)

  - Does the default setting work for achieving the purpose (at least with basic functionality)?
  - Does the change of the pre-setting increase or decrease the user's privacy? To what extent? Are gradual changes possible?
  - How are users supported in changing the settings, e.g. explanation of the effects, offering typical combined settings profiles (e.g. appropriate for a chosen risk level), allowing for specific individual customisation?
  - Can the user conveniently reset the configured setting and go back to the pre-setting?
  - How is the handling of pre-settings and settings changed by the users when the system is updated? Are the previous settings maintained? How are users informed about new settings, new options, new functionality or privacy risks?

The aforementioned list of questions should not be seen as exhaustive. Moreover, as discussed earlier, other parameters also need to be considered in the selection of defaults, especially with regard to usability and security technical implementation aspects.

5. Conclusions and recommendations

The choice of defaults in software engineering is nothing new – all developers have to deal with the question of appropriate pre-settings of information and communication technology all the time. However, the principle of "data protection first", as demanded by the GDPR when it comes to data protection by default, has neither been the standard behaviour of products, services and application nor a regular principle in software design methods.

The power of defaults is widely acknowledged. To this end, GDPR asks for data-protection-friendly pre-settings for processing of personal data. Those defaults constitute the initial configuration of the data processing. According to GDPR, for each purpose of data processing, only the minimum amount of personal data should be processed, the processing should be minimal, the shortest period of storage should be chosen, and the possibilities for accessing the personal data should be minimised as well. This means that the starting point for the data processing is based on the necessity principle. Anything in addition to what is necessary for the purpose would require an active intervention by the user, e.g. to give consent for providing more personal data or allowing additional ways of processing.

Thus, the objective of data protection by default is to ensure the fundamental principles of data minimisation and storage limitation in the IT systems – at least in the beginning when the user has not changed the pre-installed settings. This is a means to minimise the risk of data processing for the respective purpose; no unexpected data processing takes place. This contributes to the GDPR's goal of fairness of processing personal data. It can also contribute to other important GDPR provisions, such as the security of personal data processing.

However, the reality is different. It has been shown numerous times that products, services and applications in real life often do not put data protection first, but – on the contrary – process data that are strictly speaking not necessary for the communicated purpose and have not reduced the data processing to the least extent possible [Forbrukerrådet, 2018] This would not only encompass the primary functionality of data processing and the related data values, but shows interdependencies with the modalities of data processing, e.g. if temporary files are employed, if data are transferred to remote services or if log file entries are created.

This report has shed some light on what the data-protection-by-default principle means in information technology design. The compiled guiding questions bear the potential to support data controllers as well as producers of products, services and applications to achieve data-protection-friendly default settings. Still, several aspects of the data protection by default will have to be discussed more thoroughly in the future, and appropriate best practice solutions should be made more visible. Analysing the interplay between data protection and security defaults is also essential to this end, taking also into consideration relevant usability aspects. To this end, the report is a stepping stone to the broader discussion for security and privacy defaults in online systems and services in the future.

In the following Sections, we summarise several of the identified open issues and provide relevant recommendations.

5.1 Recommendations for data controllers and producers

The GDPR demands that data controllers realise data protection by design and by default in their data processing. This means that each data controller has to check whether this demand is sufficiently fulfilled. For the default requirement it means to make sure that appropriate pre-settings – according to the principle "data protection first" – have been chosen. In case the employed products, services or

applications do not allow for data-protection-friendly default settings, the data controller should convey this demand to the producers or the data processors. It may be advisable to formulate the condition "data protection by design and by default" in any procurement procedures and use this criterion for selecting the suitable products, services or applications. Clearly, joint actions by controllers (e.g. in specific industry sectors or in the public domain) can have stronger impact on producers, while also being more economically viable for the controllers.

Data con*trollers should make the notions of 'by design' and 'by default' key building blocks of their data processing operations and invest in relevant best practice implementations.*

Producers are not directly addressed by the GDPR, but if their products, services and applications can be used for processing personal data in Europe, it is certainly recommendable to fulfil the requirement of "data protection by design and by default" and document how it is implemented. This documentation can be handed over to data controllers so that they can add it to their accountability documents and thereby can be sure to meet the GDPR requirement. An exemplary realisation including the accompanying information can be a competitive advantage for products, services and application. The integration and interplay with security defaults is also important in this regard.

Producers should also invest in teaching and advising the development team in data protection by design and by default. The development process should take into account data protection principles throughout the entire process. For the default settings, the decisions need proper reasoning and justification that should be documented. Specific milestones in the development process could be dedicated to checks for appropriate pre-settings; the testing procedures should diligently tackle these aspects, too.

Further, specific protection tools could be envisaged that help users or data controllers in changing potentially data-protection-unfriendly pre-settings before the usage – for users, this could be a do-it-yourself protection approach, for data controllers it would enable them to better fulfil the data-protection-by-default principle. Also, during the usage of a product, service or application, specific tools may support filtering personal data or blocking any exuberant processing to limit the processing to the extent necessary.

Producers of products, services and applications should refrain from using design patterns that can lead users towards non-privacy friendly choices; On the contrary, they should embed security, as well as data protection by design and default into their business models and provide adequate guidance and support to data controllers and end-users.

5.2 Recommendations for end-users

Currently, many products, services and applications have not taken the data-protection-by-default principle into account when designing the IT systems. So end-users cannot rely on a data-protection-friendly pre-setting (and in many cases not even in a secure by default pre-setting). For their own protection, end-users should check the configuration and the options to change the settings. Also, they can inform the data controller about their impression of insufficient defaults and ask for improvement. According to the GDPR they have the right to lodge a complaint with a supervisory authority. Also, consumer protection organisations can support them in exercising their rights.

End users should seek to understand the security and data protection options and configurations of the products, systems or applications they use; they should inform themselves about their rights under the data protection (as well consumer protection) legislation.

5.3 Recommendations for regulatory bodies

The supervisory authorities could clarify their expectations on how to translate the requirement of data protection by default into action. This could be done by joint opinions or guidelines issued by the European Data Protection Board. Further, pointers to examples will help to distinguish acceptable or even exemplary practices from unacceptable default settings. This may help in achieving the level playing field for all actors that is promoted – but not yet existent – by the GDPR.

A more detailed interpretation of the provisions in the GDPR will also be expedient for all certifications that will be conducted on basis of Article 42 of the GDPR: Presumably data protection by default will be a criterion that has to be checked for all certification procedures. This also means that it would be helpful to give advice or set requirements on how to demonstrate that the appropriate pre-settings have been chosen and how this should be tested by certification bodies. This is particularly interesting in complex situations if different settings could qualify for a good data-protection solution.

Since the fulfilment of the data-protection-by-default principle has to be determined for each specific purpose, this poses the question how the purposes are determined and which granularity of purposes is acceptable. For example, the purpose “online shopping” is composed from several phases that may also constitute fine-granular purposes which have an impact on the necessity of data or processing operations: e.g. “online browsing”, “choosing products”, “payment”, “delivery”, “return delivery”, “issuing review comments”, “age verification” (or other limiting criteria) in case of special products, “personalised advice”, “advertisement” etc. Depending on the choice of technical means including privacy technologies, the necessity can further change. If possible, it should be clarified what the requirements with regard to data protection defaults are.

In addition, as data protection is not the only principle to consider with regard to defaults, it is essential to examine its interplay (in specific use cases) with other essential principles, such as its correlation with security defaults, as well as its interplay with usability requirements.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should provide further guidance on the notion and practical implementations of defaults; they should also present best practice examples and relevant use cases that can be used by the data controllers (as well as the producers of products, services and applications) who seek to meet the GDPR requirements.

5.4 Recommendations for policymakers and standardisation bodies

The principle of data protection by default should be considered by lawmakers and standardisation initiatives when it comes to processing of personal data. In the interest of clarity, legal and technical norms should be explicit on default settings whenever this is applicable. If possible, they also could make clear which data-protection-unfriendly default settings should be avoided.

Naturally, these clarifications should be based on the necessity principle and thereby avoid to demand for an excessing amount of personal data or of processing. In world-wide standards, not only the GDPR would have to be considered, so potential data-protection-friendly defaults may not be fixed for all fields of application. However, in these cases there should be solutions for the European market for processing personal data so that appropriate defaults could be set by the controller.

Again, a combined approach for data protection by design and data protection by default would be promising instead of only focusing on the best pre-setting since from the technical perspective the necessity can be dependent on the choice of technical and organisational measures for building in data protection. The dimension of security defaults is also essential to consider to this end.

Policy makers and standardization bodies should support the adoption of the data protection by default (as well as by design) by proposing, wherever possible, relevant technical norms and solutions, as well as considering its correlation with the notion of security by default.

5.5 Recommendations for the research community

For researchers, the data-protection-by-default debate provides multiple interesting angles: Certainly several open questions hamper data controllers in implementing appropriate pre-settings– or even in formulating what they demand from producers. A simple question that is hard to answer is the comparison of data-protection-quality between different possible defaults. Although the provision in the GDPR contains four criteria, there is no accepted metrics for an easy comparison. For several options it may be obvious what is better and what is worse, but there may be differences according to the chosen technologies. Also different user groups may call for different pre-settings, e.g. if specific protection levels have to be considered as it may be the case for minors.

If data protection by default is taken seriously, many known and widespread products, services and applications may have to be changed. This may affect those business models that profit from excessively analysing personal data that users would not disclose only for the original purpose (and where they often are not aware of). Data protection by default may question the model of payment by divulging personal data.

Here, certain parties may become creative in defining purposes where data minimisation is hardly possible, as well as use psychological tricks to direct people towards disclosing more data or allowing more data processing. This potential effect constitutes an own research topic: to identify possible circumvention schemes or approaches to discredit the data-protection-by-default principle. On a practical side, it would be interesting how to detect unfair purpose definitions, data processing defaults and change options.

What is more, the principle of “data protection first” may mean to put other valuable principles second, e.g. ecological sustainability, democratic participation or support of minorities. It may be taken up by research whether the implementation of other important principles should also be pushed. To this end, the notion of ‘security defaults’ (and its interplay with data protection defaults) is of particular relevance and a field for further work in the future.

For upcoming technologies research should elaborate possible solutions for data protection by design and by default to reduce the risk of misuse of personal data and to other rights and freedoms. This should take into account also security aspects, as well as issues of usability, transparency and inclusion.

The research community should continue working on the notion of data protection by default, especially in correlation with security and usability, as well as other interdisciplinary principles that govern defaults; they should also analyse new online business models based on security and privacy defaults, as well as technologies that can facilitate their adoption.

6. References

Acquisti, L. K. John, G. Loewenstein, *"What Is Privacy Worth?",* The Journal of Legal Studies, Vol. 42, No. 2, pp. 249-274, 2013.

Angulo, J., Fischer-Hübner, S., Wästlund, E., Pulls, T.: *Towards usable privacy policy display and management*. Inf. Manag. Comput. Secur. 20(1), 4–17, 2012.

Article 29 Data Protection Working Party, *"Opinion 8/2014 on the Recent Developments on the Internet of Things",* 14/EN, WP 223, 2014. (WP29, 2014a)

Article 29 Data Protection Working Party, *"Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting",* 14/EN, WP 224, 2014. (WP2019, 2014b)

F. Bieker, M. Hansen, *"Datenschutz „by Design" und „by Default" nach der neuen europäischen Datenschutz-Grundverordnung",* RDV 2017, pp. 165-170, 2017.

L. A. Bygrave, *"Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements",* Oslo Law Review Vol. 4 Nr. 2 (2017), pp. 105-120, 2017.

A. Cavoukian, *"Privacy by Design – The 7 Foundational Principles",* 2009, revised 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

S. Chitkara, N. Gothoskar, S. Harish, J. I. Hong, Y. Agarwal, *"Does this App Really Need My Location? Context-Aware Privacy Management for Smartphones*", Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 1, 3, Article 42, 2017.

Datatilsynet, *"Software development with Data Protection by Design and by Default",* 2018, https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/.

ENISA, *"Privacy and Data Protection by Design – from policy to engineering",* 2014.

ENISA, *"Privacy by design in big data"*, 2015.

ENISA, *"Privacy and data protection in mobile applications – A study on the app development ecosystem and the technical implementation of GDPR",* 2017.

European 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), 2017.

European Council, *"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)",* 8537/18, 2018.

European Data Protection Supervisor (EDPS), *"Opinion of the European Data Protection Supervisor on the data protection reform package,"* 2012.

European Data Protection Supervisor (EDPS), *"Opinion 5/2018 – Preliminary Opinion on privacy by design",* 2018.

R. T. Fielding, D. Singer, D. (eds.), *"Tracking Preference Expression (DNT)",* W3C Candidate Recommendation, 2017, http://www.w3.org/TR/tracking-dnt/.

Forbrukerrådet (Norwegian Consumer Council), *"Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy",* 2018.

Forbrukerrådet (Norwegian Consumer Council), "Every step you take - How deceptive design lets Google track users 24/7", 2018. (Forbrukerrådet, 2018 -1)

M. Hansen, *"Data Protection by Default in Identity-Related Applications",* in: Proc. IDMAN 2013, IFIP AICT 396, pp. 4-17, 2013.

M. Hansen, *"Data Protection by Design and by Default à la European General Data Protection Regulation",* in: A. Lehmann et al. (eds.): Privacy and Identity Management – Facing up to Next Steps, Proc. IFIP International Summer School on Privacy and Identity Management, IFIP AICT vol. 498, Springer, pp. 27-38, 2017.

M. Hansen, *"Artikel 25 DSGVO (Article 25 GDPR) – commentary",* in: Simitis, Hornung, Spiecker gen. Döhmann, Datenschutzrecht: DSGVO mit BDSG, Nomos, 2018.

Information Commissioner's Office (ICO), *"Data protection by design and default",* 2018, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

International Working Group for Data Protection in Telecommunications, *Working paper and recommendations on the publication of personal data on the web, website context indexing and the protection of privacy*, 2013. (IWGDPT, 2013)

International Working Group for Data Protection in Telecommunications, Connected Vehicles, 2018, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Connected_Vehicles.pdf (IWGDPT, 2018).

E. J. Johnson, S. Bellman, G. L. Lohse, *"Defaults, Framing and Privacy: Why Opting In-Opting Out"*, Marketing Letters, 13: 5, 2002.

P. A. Keller, B. A. Harlam, G. Loewenstein, K. G. Volpp, *"Enhanced active choice: A new method to motivate behavior change",* Journal of Consumer Psychology Vol. 21 No. 5, pp. 376-383, 2011.

J. P. Kesan, R. C. Shah, *"Setting Software Defaults: Perspectives from Law",* Computer Science and Behavioral Economics. U Illinois Law & Economics Research Paper No. LE06-012. Notre Dame Law Review 82, pp. 583-634, 2006.

P. G. Leon, B. Ur, R. Balebako, L. F. Cranor, R. Shay, Y. Wang, *"Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising",* in: Proc. CHI '12, pp. 589-598, 2012.

M. Madejski, M. Johnson, S. M. Bellovin, *"The Failure of Online Social Network Privacy Settings",* Tech Report CUCS-010-11, Columbia University, 2011.

Ravichandran, R., Benisch, M., Kelley, P.G., Sadeh, N.M.: *Capturing social networking privacy preferences: can default policies help alleviate tradeoffs between expressiveness and user burden*? In: Goldberg, I., Atallah, M.J. (eds.) PETS 2009. LNCS, vol. 5672, pp. 1–18. Springer, 2009.

L. Olejnik, G. Acar, C. Castelluccia, C. Diaz, *"The leaking battery – A privacy analysis of the HTML5 Battery Status API"*, in: Revised Selected Papers of the 10th International Workshop on Data Privacy Management, and Security Assurance, Vol. 9481, pp. 254-263, 2016.

R. Thaler, C. Sunstein, *"Nudge – Improving decisions about health, wealth and happiness",* 2008.

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number TP-03-18-573-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-285-1
DOI: 10.2824/518496