Privacy & Us

D5.1 Privacy Principles

Deliverable Number	5.1
Work Package	WP5
Version	0.6
Deliverable Lead Organisation	ULD
Dissemination Level	PU
Contractual Date of Delivery (release)	31 July 2017
Date of Delivery	31 July 2017
Status	**FINAL**

Editor

Alexandr Railean (ULD)
Harald Zwingelberg (ULD)

Contributors

Luiza Rezende (TAU, ESR 9)
Alexandros Mittos (UCL, ESR 11)
Majid Hatamian (GUF, ESR 5)
Lamya Abdullah (UNI, ESR 10)
Agnieszka Kitkowska (KAU, ESR 2)
Alexandr Railean (ULD, ESR 6)
Harald Zwingelberg (ULD)

Reviewers

Michael Bechinie (USE)
Leonardo Martucci (KAU)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

European Commission

Executive Summary

This report is part of a series planned within work package 5 “Risk analysis, Risk Perception and Law” of the Marie Skłodowska Curie innovative training network Privacy&Us. Thirteen early stage researchers (ESR) will be trained to face both current and future challenges in the area of privacy and usability as part of their PhD-programme. Work package 5 fits into this by integrating several ESRs in the process of preparing a privacy risk analysis. This project report (D5.1) kicks off the work, lays the foundation for this planned series of reports and addresses the relevant aspects of privacy and usability:

D5.1 Privacy Principles
D5.2 Risk Assessment
D5.3 Risk Mitigation
D5.4 Risk Awareness Creation

The contributions are oriented on the topics that are addressed by the ESRs and identify the protection targets on basis of the SDM.

In respect to the GDPR, this report exemplifies that usability aspects will be more important for data protection compliance in the future. The definition of usability according to ISO 9241-210:2009 is "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.” The data protection goal of transparency is closely related to such aspects. As transparency requirements had been sharpened in the GDPR, e.g. the regulation now clearly demands that declarations must be presented in an easy language. To effectively provide the information necessary according to the GDPR data controllers need to consider such concepts in broad. Where possible the capabilities of user interfaces to communicate with audio and voice or haptic feedback should be considered. Likewise the accepted practices for accessibility should be adhered to, allowing better access to e.g. vision impaired and easing the difficulty of reading texts. Likewise this could be stipulated for the enforcement of data subjects’ rights which should be easy to accomplish or at least not too complex to enforce.

However, not only the law became stricter but also the systems and processes become more complex. It poses a challenge to understandably explain processes and data flows involved in cloud computing. In the field of IoT one often faces devices missing input and output devices such as a screen forcing to recourse to external devices.

Table of Contents

1 Introduction

This report is part of a series planned within work package 5 “Risk analysis, Risk Perception and Law” of the Marie Skłodowska-Curie innovative training network Privacy&Us. Thirteen early stage researchers (ESR) will be trained to face both current and future challenges in the area of privacy and usability as part of their PhD-programme. Work package 5 fits into this by integrating several ESRs’ topics in an exercise creating privacy risk analyses or relevant parts thereof. This project report (D5.1) kicks off the work, lays the foundation for this planned series of reports and addresses the relevant aspects of privacy and usability:

D5.1 Privacy Principles
D5.2 Risk Assessment
D5.3 Risk Mitigation
D5.4 Risk Awareness Creation

The contributions are oriented on the topics that are addressed by the researchers: cloud computing in relation to smart environment (ESR 2), cloud computing and attitudes towards privacy (ESR 10), the processing of genomic data (ESR 11), privacy in smartphone environments (ESR 5) and the privacy aspects raised by the Internet of things (ESR 6). The ESRs responsible for these technology-oriented topics identified the protection targets in their respective application domain. Based on their input, ESR 9 with a focus on legal and data protection aspects provided an introductory legal section. The considerations on protection targets where extended with pointers to specific legal concerns by Privacy&Us project partner ULD.

The work follows the privacy impact assessment (PIA) methodology. However, since the planning phase of the project the European General Data Protection Regulation (GDPR) has been ratified and entered into force – to be directly applied as of May 2018, this provided a major change in the legal setting. For the sake of later usefulness, all evaluations are done on basis of the GDPR, however, with the risk that the researches faced the problem still unpublished literature and jurisprudence – a broader set of secondary literature on the GDPR had not been available on the market until late spring 2017 and there mainly the German speaking legal community was addressed.

With uptake of the GDPR, also our terminology underwent a change: instead of following the privacy impact assessment (PIA) methodology, we base our outline on the data protection impact assessment (DPIA) as set forth in Art. 35 GDPR. For this, a unified methodology or framework has not been agreed on yet. The Art. 29 Data Protection Working Party identified in its working paper[1] four EU generic frameworks for DPIA. This report follows the approach supported by the German data protection authorities: the “Standard Data Protection Model” (SDM) (see below chapter 2).[2]

The Standard Data Protection Model and the protection goals which will be used as structure for the identification of protection targets are summarized in chapter 2. A more detailed legal perspective of the protection goals with light shed specifically to aspects of interest for usability is set forth in chapter 3. Chapter 4 is the core of this document, identifying the protection targets for the specific topics of the ESRs in individual sub chapters. The report is rounded up by a summary and outlook in chapter 5.

[1] Art. 29 WP 248, p. 20.
[2] DSK, SDM p. 3 et seq.

2 The Standard Data Protection Model

The Standard Data Protection Model will in this report be deployed to identify the protection targets by using utilising the protection goals of the model as privacy principles. The underlying model of protection goals historically leads back to the confidentiality – integrity- availability –triad developed and well accepted within computer security domain e.g. in the ISO 27xxx –series. Originating from this Rost and Pfitzmann developed and extension with a triad of data protection goals. [3] Also the pre-existing triad was extended with considerations stemming from data subjects basic rights as so far IT-security had primarily be seen in the light of protecting the assets of organisations. This system evolved and had been applied in the practical work of German data protection authorities (DPA) and for structuring considerations in research reports. The system has the support of the Conference of the Independent Data Protection Authorities of the Bund and the Länder (DSK)[4] in Germany in November 2016.[5] A English translation of SDM is available since March 2017.[6] The SDM has been listed by the Art. 29 Data Protection Working party as one of the potential model to apply for data protection impact assessments.

The three data protection goals are: transparency, intervenability and unlinkability (The principle of data minimisation is both part of Unlinkability but must also be considered before assessing on basis of the SDM and therefore follows a double role.) The all six protection goals together cover the relevant aspects of both ICT-security and data protection. In a graphical representation the typical conflicts between the goals that need active decisions in the development of processes are displayed (figure 1).

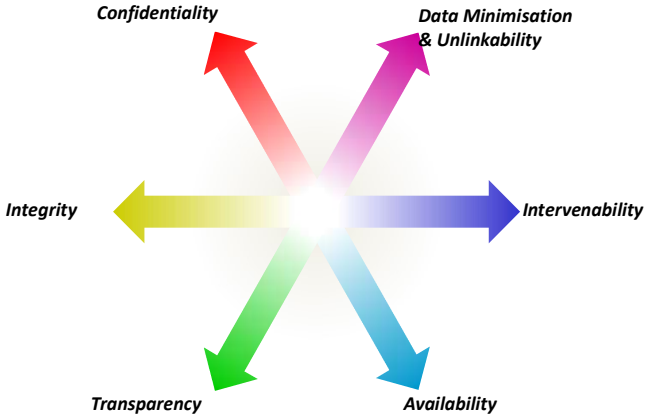

Figure 1. The data protection goals.

The protection goal **unlinkability** refers to the requirement that data be processed and evaluated only for the purpose for which they are collected.[7] Processing of personal data for other purposes than the one for which the data has initially been collected is allowed only under strictly defined circumstances. Data subjects whose data are processed for further purposes can be protected by measures taking the linkability of these data from the identity of the natural person to the extent possible, e.g. by the measures of pseudonymisation and anonymisation.

The protection goal **transparency** "refers to the requirement that the data subject as well as the system operators and the competent supervisory authorities can identify to a varying extent, which data are collected and processed for a particular purpose, and which systems and processes are used for this purpose, where the data flow to which purpose, and who is legally responsible for the data and systems in the various phases of data processing."[8] To be operated lawfully transparency is necessary throughout a system lifecycle. E.g. transparency is necessary in relation to data subjects to obtain informed consent but also to fulfil the firmed transparency and publicity requirements in Art. 12 et seq. GDPR. In relation to DPAs a well-kept and up-to-date documentation of systems and impact assessments can demonstrate an accountable operation of systems. Transparency is highly relevant within Privacy&Us, as interfaces that had been developed under respect of the principles of human

[3] Rost, Pfitzmann, p. 354 et. Seq.
[4] Privacy&Us beneficiary ULD is a member of the DSK and propagated the SDM in the past. LDA Bayern is the Bavarian DPA and associated to Privacy&Us. In December 2016 the SDM was unanimously and affirmatively acknowledged by the DSK under abstention of LDA.
[5] DSK, SDM.
[6] Online: https://www.datenschutzzentrum.de/SDM/
[7] DSK, SDM p. 13.
[8] DSK, SDM p. 13.

centered design may aid controllers to fulfil the high demands yet better. E.g. a first step is providing a solution for having short and understandable but still sufficiently informative privacy declarations delivered to data subjects which then can be refined to address further user needs.

Finally the "protection goal **intervenability** refers to the requirement that the data subjects are effectively granted the right to notification, information, rectification, blocking and erasure at any time, and that the processing body is obliged to implement the appropriate measures. For this purpose, the authorities responsible for the processing must be able to intervene in the processing of data from the collection to the deletion of the data."[9] Well-thought usability may help to leverage the data subjects' rights by providing easy means to manage the behavior of systems, e.g. the rights for smartphone apps or limits for the physical location of data in cloud environments.

The existing protection goals known in the ICT-security field gain some specific accents when viewed from a basic rights perspective rather than from protecting assets of an organisation.

Confidentiality is mainly implemented by technical and organisational measures as demanded in Art. 32 GDPR. Further measures may become necessary where the assessment concluded that confidentiality falls into the protection categories high or very high protection and consequently demands more measures to be taken. Confidentiality aspects should be thought about right from the beginning of planning and setting up a process. Likewise aspects of usability should be taken into account. A clear UI and good explanation may help to understand protection measures. Such well elaborated and understandable features are also less likely to annoy users avoiding the potential consequence to be deactivated or circumvented.
Likewise data protection by default plays a role for usability considerations. Defaults should be privacy preserving, e.g. checkboxes allowing certain additional processing steps must not be pre-checked thus asking for active opt-in to allow processing than demanding users to take action to opt-out to get the option processing less personal data. Good user guidance may also help to solve a practical problem where additional services require additional processing and thus is subject to informed consent of the user. In these cases the data protection by default paradigm requires that first the legal ground is clarified by consent and then the processing being necessary part of the service may take place as necessary part of the service the user opted for. Ideally the additional necessary data for such a service and the consent can be displayed transparently and consent obtained with a single action confirming the new setting.

Aspects of **integrity** are addressed in the GDPR (Art. 5 (1) (f) GDPR), stipulating that personal data processed should remain intact, complete and up-to date. Under data protection aspects it is of interest that personal data is not changed in a way that may allow discrimination or cause other negative effects for the data subjects including a change of the context the data.

For data protection aspects of **availability** are rather of a subordinate role. In the total overview of the protection goals availability often is directly linked to the interests of the controller as a functioning data processing may be vital for the business interests pursued. In the field of data protection availability is usually of less importance to the data subject unless services directly benefit life and health of a data subject (e.g. electronic health records) the protection category for availability usually is normal and even a delay of several days in respond to a right to access or right to rectification request lies well within acceptable timeframes. In short: Availability of the services is usually a concern of the controller. As for processes enabling data subjects rights these must be defined and in place but are mostly not so time critical as to require specific technological or organisational measures.

The model comes in play for the data protection evaluation of processes. In general every processing of personal data requires a legal ground which must be identified already.

Each processing of personal data requires a valid legal ground to be in place according to Art. 6 (1) GDPR where "processing shall be lawful only if and to the extent" that one of the permissions set forth in that article apply. Of great practical importance is informed consent and processing which is necessary for the purposes of legitimate interests according to Art. 6 (1) (a) and (f) GDPR. Where

[9] DSK, SDM p. 13.

more than one legal ground applies, the controller has the right to decide which legal ground the processing will be based on.[10]

Once the legal ground is identified the model is applied to identify the protection targets, the required level of protection and provides pointers to potential measures to mitigate existing risks. Depending on the legal ground there may be a close interplay between the legal ground, risks for protection goals and mitigation methods, e.g. when according to Art. 6 (1) (f) GDPR processing is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject […]". In this case the processing may not be permitted unless certain specific measures are taken to sufficiently mitigate risks for the rights and freedoms of the data subjects. The model allows systemizing the measures on the basis of the protection goals.[11]

Finally it should be stated that all considerations done in basis of the SDM can easily be linked to legal requirements. While the model has been developed under the German Data Protection Act based on the old data protection Regulation 95/46/EC all concepts had been derived from the legal texts.[12] As the core principles remained mainly unchanged or have been even tightened and refined in the case of transparency a mapping is easily possible also for the legal acts to be applied as of May 2018.

[10] Buchner, Petri in Kühling, Buchner (eds.), Art. 6 DSGVO para. 22.
[11] DSK, SDM p. 6.
[12] See DSK, SDM p. 19 et seq. for a mapping to the Federal Data Protection Act and p. 21 et seq for a mapping to the data protection laws of the German federal states with the a mapping-table for the Saxon Data Protection Act.

In an overview the articles of the GDPR map to the SDM protection goals as shown in the Table 1.

Table 1 Allocation of the articles of the GDPR to the Protection Goals[13]

Data minimization	Availability	Integrity	Confidentiality	Unlinkability	Transparency	Intervenability
5 I c), 5 I e), 25, 32	5 I e), 13, 15, 20, 25, 32	5 I f), 25, 32, 33	5 I f), 25, 28 III b), 29, 32	5 I c), 5 I e), 17, 22, 25, 40 II d)	5 I a), 13, 14, 15, 19, 25, 30, 32, 33, 40, 42	5 I d),5 I f), 13 II c), 14 II d), 15 I e), 16, 17, 18, 20, 21, 25, 32

Likewise the articles of the Directive (EU) 2016/680 (Police Data Protection Directive)[14] applicable to data processing for purposes of the prevention, investigation, detection or prosecution of criminal offences can be mapped to the protection goals (see Table 2).[15] The general data protection rules apply there alike. However, due to the specific area of application the legislator has already anticipate the weighing test for a series of use cases allowing the competent authorities specific types of processing directly or very invasive types of processing on basis of a court order.

Table 2 Allocation of the articles of the Police Data Protection Directive to the Protection Goals

Confidentiality	Integrity	Availability	Unlinkability + Data minimisation	Transparency	Intervenability
4 p. 1 (f) 5 8 9 20 22 p. 3 (b) 29	4 p. 1 (d), (f) 6 7 20 p. 1 24 25 29	4 p. 1 (f) 12 13 14 20 p. 1 29	4 p. 1 (b) - (f), p. 2 (a), (b), p. 3 5 8 9 20 29	4 p. 4 13 14 17 p. 3 19 p. 1 20 24 25 28 30 31	4 p. 1 (d) 11 p. 1 + 2 12 p. 2 13 14 (e) 16 17 18 20 22 p. 3 (d)

[13] Source: DSK, SDM p. 25.
[14] Directive (EU) 2016/680 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 competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN.
[15] Based on unpublished work by Schehahn, for VALCRI project funded by the European Commission. VALCIR white paper to appear 2017, Project website: http://valcri.org/.

3 Legal setting

As of May 25th 2018 the General Data Protection Regulation (GDPR) will be the main legal privacy framework in the European Union. When compared to its predecessor, the Data Protection Directive 95/46/EC which is replaced by the regulation, the GDPR brought multiple changes that will also affect the field of usability; some of the relevant changes are clarified below. In the next section, the GDPR principles belonging to the Standard Data Protection Model as proposed by the Conference of the Independent Data Protection Authorities of the (German) Bund and the Länder and reflecting important protection goals (confidentiality, availability, integrity, transparency, unlinkability, intervenability) will be further explained.

First of all, the GDPR as a regulation will be directly applicable to all member states, without the need for national implementation, as it is for directives such as for Directive 95/46/EC. Also, the GDPR will be applicable when data from people located in the European Union is processed, even if the processing occurs outside the Union and the data controller is not located within the Union, which makes the GDPR broadly applicable, surpassing geographical barriers.[16] The GDPR introduces new principles and accentuates existing principles in particular regarding transparency, understandable information of the data subjects including plain language but also require certain information to be provided. Usability professionals must therefore be constantly aware of the new principles which may influence in their area of expertise e.g. with the detail and type of information that must be provided by user interfaces. The rules instituted by the GDPR will be directly applicable to all activities in the context of an establishment in the EU and may also be subject to enforcement of entities outside EU borders under the conditions of Art. 3 (2) and (3) GDPR.

There are also relevant changes regarding the need for informed consent and its validity requirements. The basic definition given by the GDPR is that consent means “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.[17] So far there are still doubts on how to implement mechanisms of consent that can comply with all the requirement listed in this definition and in the other articles of the GDPR that deal directly with consent.[18] Usability professionals will have the cope with this challenge, implementing consent processes that fit the overall GDPR protection model and that meet the specific consent requirements set by the legislation. Specific challenges arise where there are only little or highly limited means to communicate with the data subject e.g. in the field of mobile apps, where at least a display exists and the area of IoT where recourse needs be held to external devices (see Section 4.3 for smartphone ecosystems and Section 4.4 for specifics of IoT).

Another important element of the new conception of informed consent is that “the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.”[19] It means that, in case of conflict, the burden of proof of the adequacy of consent lies on the controller, something that was not expressly mentioned in the previous framework. When designing a structure for consent in an information system, usability professionals will have to keep that in mind, as the controller has to be able to prove that consent was adequately obtained.

Data protection by design and data protection by default are now in the centre of the data protection model – as explicitly established by Art. 25 and recitals 78 and 108 of the GDPR. These principles should be fully in all the work phases. Where special attention is given to aspects of usability and interface design during development the necessary information may even be better communicated or even become understandable for the data subjects addressed in the first place. The basic requirements related to the security of the processing that have to be ensured by data controllers and processors are contained in Art. 32 GDPR.

[16] See Art. 3 of the GDPR – Territorial scope. Also Warwick Ashford, *10 key facts businesses need to note about the GDPR*, COMPUTER WEEKLY, 13 May 2016 (last visited on April 28th 2017), at http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR.
[17] Recital 32 and Art. 4 (11) of the GDPR.
[18] For example Art. 7, 8 and 9 of the GDPR.
[19] Art. 7 (1) of the GDPR.

In the GDPR, data subjects' rights and data processors' obligations are more abundant and prominent than in the previous legal framework. Among the rights of the data subjects enlisted in Art. 12 et seq. GDPR are the right to information, right of access, right to rectification, right to erasure (right to be forgotten), right to restrict processing, right to data portability, right to object and the right not to be evaluated on the basis of automated processing.[20] Among the data processors' obligations are demonstrating compliance, security, breach notification, data protection officers and codes of conduct.[21] Again, usability professionals will have to be aware of these rights and obligations to be compliant with the GDPR, and will have to structure systems that are compliant with the new rules.

Until the enforcement date of the GDPR (May 25th 2018), the current framework - the Data Protection Directive 95/46/EC – is still applicable, as well as the national laws that were established in accordance with it. When enforceable, as we saw, the GDPR will not require national implementation, however, some opening clauses will allow national specifics to be regulated. Despite the intra-EU harmonization sought by the GDPR, there might be divergences in the interpretation of the GDPR's precepts by different Union Members' courts and in the way national laws will be amended to follow the GDPR model unless relevant cases become subject to preliminary rulings of the European Court of Justice. The analysis of these national divergences will be pending until after May 2018, until court decisions start being issued.

The GDPR covers the processing by public and private entities alike. Where personal data is processed by "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" the GDPR does not apply but the national implementation of Directive 2016/680/EU.[22] However, as also the directive follows the basic principles of data protection for the protection of basic rights findings done on basis of the SDM should in most cases match also for in the field of application of the directive. A mapping table of articles of the regulation to the SDM has been proposed

In the following subsections the relevant legal norms and main considerations of the GDPR with relevance to usability and the topics addressed by the ESRs are introduced sorted by data protection goals:, Confidentiality (3.1), Availability, (3.2), Integrity (3.3), Unlinkability (3.4) Transparency and Intervenability (3.6).

3.1 Confidentiality

Data and services that process such data cannot be accessed by unauthorized entities

Relevant legal norms of the GDPR
Confidentiality is an important principle for processing of personal data, and important provisions are brought by Art. 5 (f), 25, 28 (3) (b) and 32 (1) (b) GDPR:

- *Art. 5. "Personal data shall be: […] (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"*
- *Art. 25 (1) "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the*

[20] For an oversight cf. Tim Hickman & Detlev Gabel, *Rights of Data Subjects under the GDPR, SOCIETY FOR COMPUTERS AND LAW'S WEBSITE*, (last visited on April 28th 2017) https://www.scl.org/articles/3575-rights-of-data-subjects-under-the-gdpr.
[21] Heywood 2016.
[22] Directive (EU) 2016/680 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 competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

- *(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. […]"*
- *Art. 28 (3). "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: […] b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; […]"Art. 32 (1) "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;"*

Comments

From the stated above, we see that some of the concerns raised by ESRs are directly supported by the legal stipulations of the GDPR:

- Privacy attitudes and behaviours in the cloud: *multitenancy* and *outsourcing* were enumerated as possible threats. In both cases these relationships should be governed by adequate contractual provisions that include specific clauses protecting confidentiality of data and appropriate safety measures (both organizational and technical) to be taken by both parties. *Encryption* is a technical measure to be taken, but supporting organizational measures to help protect confidentiality should also be taken.
- Privacy in smartphone ecosystems: technical security measures were listed in order to protect confidentiality. Also, in this case, it is necessary that the multiple service providers that interact in the mobile context have contractual and organizational safeguards to protect confidentiality.
- For the smartphone ecosystems: Any data in transfer should be properly protected, e.g. by encryption. Generally for the measures taken must be sufficient for the identified required protection category[23] (normal, high, very high). For the telecommunications field this is specifically important e.g. regarding content of communication but also any communication metadata granting insights into social relations or location data allowing behavioural profiles may be very sensitive.

[23] DSK, SDM p. 34.

- Usable privacy in the internet of things and smart spaces: the issue of organizational threat posed by dishonest employees was raised. According to Art. 28 (3) (b), 32 (1) (b), the appropriate contractual and organizational measures shall be taken to protect confidentiality, including those that involve authorized employees, contractors and third parties.
- Genomic privacy: immutability of genomic data was brought up as an aggravating situation. Suitable contractual and organizational measures shall be taken to reduce the risk (besides technical measures, such as encryption).

3.2 Availability

Access to (privacy-relevant) data and to services that process such data is always granted in a comprehensible, processable, timely manner.

Relevant legal norms of the GDPR. The relevant GDPR articles are 13 15, 20 and 32. Art. 15 of the GDPR deals with the right of access by the data subject:

- *Art. 15 (1)" The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*
  (a) the purposes of the processing;
  (b) the categories of personal data concerned;
  (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
  (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
  (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
  (f) the right to lodge a complaint with a supervisory authority;
  (g) where the personal data are not collected from the data subject, any available information as to their source;
  (h) the existence of automated decision-making, including profiling, referred to in Art. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
  2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Art 46 relating to the transfer.
  3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
  4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

Comments
From the stated above, we see that some of the concerns raised by ESRs are supported by the legal stipulations of the GDPR:

- Privacy attitudes and behaviours in the cloud: threats related to outsourcing, training, end-user issues and storage limitations were brought. It should be noticed that the GDPR requires the

availability of different categories of information about the collected data (Art. 15 (1) items a-h), so the organization has to be prepared to offer them to the end user, enabling him or her "to exercise that right easily and at reasonable intervals" (recital 63).

- Privacy in smartphone ecosystems: the need of optimizing approaches in order to decrease the time of processing was mentioned. On that point, it is relevant to notice again that Art. 15 (1) of the GDPR enumerates a list of information about the data, what might not be easily gathered and presented to the end user in the context of smartphones. Organizations have to be aware of that legal requirement.
- Usable privacy in the internet of things and smart spaces: the challenge is similar to the one faced in the smartphone context: there is a continual and ubiquitous, data collection, from multiple sources and formats, not so easily gathered and presented to the end user. Art. 15 (1) of the GDPR imposes multiple categories of data that should be readily available and ready for presentation, what might pose challenges to the IoT context. Providing the transparency information and also the documentation has challenges as the IoT also consists of very small devices which should not be shipped with big books. Here digital (CD, DVD, USB-Stick) or online resources may be a solution that is both commercially feasible and usable.
- Genomic privacy: the data should be available to the data subject. Additional assurances have to be taken before making it available to physicians or health institutions, given the sensitivity of this type of data.

3.3 Integrity

Data and services that process such data cannot be modified in an unauthorized or undetected manner

Relevant legal norms of the GDPR
Art. 5 (1) (d), (f) and 32 (b) of the GDPR deal with Integrity of data:

- *Art. 5 "Principles relating to processing of personal data.*
  1. Personal data shall be: […]
  (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); […]
  (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
- *"Art. 32 Security of processing –*
  1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: […]
  (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;"

Comments

- Privacy attitudes and behaviours in the cloud: in case of shared infrastructure, proper organization and contractual measures should be taken in order to guarantee integrity of data (and allocate responsibilities in case of damage).
- Privacy in smartphone ecosystems: security measures that should be taken in order to avoid unlawful or unauthorized manipulation are mentioned. On this issue, also organizational and contractual measures shall be undertaken, both within the organization and between the third-parties that will have authorized access to the data.

3.4 Unlinkability and Data Minimisation

Privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context

Relevant legal norms of the GDPR Art. 5 (1) (b), (c), (e), 21(1), 25 and 32 of the GDPR are especially relevant for the unlinkability principle. Beyond that the individual legal basis for processing listed in Art. 6 GPDR apply the respective purposes followed as a benchmark for what is necessary processing and this is enacted by the purpose limitation principle in Art. 5 (1) (b) GDPR.[24] Pseudonymisation is a typical measure for unlinkability.

- *Art. 5 "1. Personal data shall be: […]*
  b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Art. 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation');
  (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); […]
  (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');"

Comments

- Privacy in smartphone ecosystems: unlinkability might be a difficult principle to implement in smartphone environments, given that in many apps the data is stored in the device and the data subject does not alter the default of the device to a more privacy preserving option. The consequence is that the device data is shared among apps, sometimes without the awareness of the user, harming both unlinkability and transparency.
- Genomic privacy: specific contractual and organizational measures must regulate the data transfer between Institutes (when authorized), so that the unlinkability principle is preserved.

[24] DSK SDM p. 25.

3.5 Transparency

All privacy-relevant data processing − including the legal, technical, and organizational setting can be understood and reconstructed at any time.

Relevant legal norms of the GDPR. The need for transparency is expressed in the GDPR in Art. 5, 12, 13, 14, 15, 19, 15, 30, 32, 33, 34, 40, 42. The articles that deal with informed consent can also be associated with the principle of transparency. Transparency reflects a fundamental principle of the new data protection legislation.

- *Art. 5 "Principles relating to processing of personal data - 1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');"*
- *Art. 12 "(1) specifically states that "The controller shall take appropriate measures to provide any information referred to in Art. 13 and 14 and any communication under Art. 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means".*

Comments

- Privacy attitudes and behaviours in the cloud: providing informed consent to process data in the cloud might be a challenge, as data subjects might not have the necessary knowledge to understand the conveyed information (what means that the consent, in the end, might not be informed as the GDPR requires). In the same way, it might be difficult to convey information about secondary uses of data to data subjects, what might put transparency in risk.
- Privacy in smartphone ecosystems: in the smartphone environment, transparency and consent might be a challenge, as many apps are constantly collecting data. It is still uncertain how frequent and how detailed should the notifications be in order to: a) properly inform data subjects about data collection and processing; b) do not interfere with the usability. There is also the challenge of what data, when and how to convey to data subjects.
- Usable privacy in the internet of things and smart spaces: the IoT scenario is maybe the one that poses more challenges to transparency and informed consent, given the different modalities of data collection, the multiple types of interfaces (not always easy to use) and the different patterns of data collection of these devices, which pose additional difficulties for conveying information in a clear, comprehensive and usable way to the data subject.
- Genomic privacy: there are peculiar risks involved in processing of genomic data, the additional challenge here is how to convey that information to data subjects in an understandable way. Moreover, some risks are uncertain and in a way unforeseeable, what raises the issue of how to convey these risks and uncertainties in a privacy notice in a way it is clear and complete enough so that the consent of the data subject might be deemed "informed.

3.6 Intervenability

Intervention is possible concerning all ongoing or planned privacy-relevant data processing

Relevant legal norms of the GDPR
Many articles in the GDPR reflect the importance of the intervenability principle (Articles 5, 12, 15, 16, 17, 18, 20, 21, 25).

- Art. 12 (2) GDPR talks about "transparent information, communication and modalities for the exercise of the rights of the data subject",
- Art. 15 (1) (e) "right of access by the data subject",
- Art. 16 "right to rectification",
- Art. 17 "right to erasure ('right to be forgotten')",
- Art. 18 "right to restriction of processing",
- Art. 19 "notification obligation regarding rectification or erasure of personal data or restriction of processing",
- Art. 20 "right to data portability",
- Art. 21 "right to object" and
- Art. 22 (3) Automated individual decision-making, including profiling.

Comments

- Privacy attitudes and behaviours in the cloud and usable privacy in the IoT: all the spectrum of rights related to intervenability (expressed in the articles enumerated supra) should not be prevented by the specific characteristic of cloud service's architecture or by characteristics such as the lack of interface in IoT environments.
- Genomic privacy: given the special sensitivity of genomic data, all existing rights related to intervenability should be made clear to the data subject.
- In the cloud, mobile and IoT, data portability might be a challenge, as Art. 20 requires that "the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format." The specific requirement of "structured, commonly used and machine-readable format" might not be easy to implement in the multiple information systems that compose cloud, mobile and IoT contexts.

4 Applying to specific sectors

In this section, the ESRs introduce their application domains and analyse the involved particular data protection related aspects. These are mapped to the data protection goals and usability specific aspects are identified. The contributions of the ESRs are seconded by legal considerations by ULD.
The goal of this section is to identify privacy principles and protection targets in the different application domains. It is the first document in a series of deliverable building up on a risk analysis aspects related to Privacy&Us (see introduction chapter 1).

4.1 Cloud computing for smart environment applications[25]

4.1.1 Smart applications

The term of smart environment covers a range of multidisciplinary research domains. It evolved over years from the pervasive computing which enables the use of different devices and technologies to provide users with smart services. It is defined as “a small world where different kinds of smart device are continuously working to make inhabitants' lives more comfortable”[26]. Smart homes, cities and spaces, etc. utilise various set of technologies such as wireless sensor networks, mobile applications, middleware and computing systems. The interaction among these technologies results in what is known as smart environment of that environment. Regardless of the specific application domain (such as, healthcare, location-based services, participatory sensing, automated homes, profiling-based shopping, etc.) the collected data in smart environment is information about most aspect of the inhabitants life, health, location, movements, and users behaviour, all are considered sensitive data. The sensor data is collected and stored for different purposes, including data analysis for decision making and service monitoring and quality control. Over the past few years, discussions have been held for the impact of such technology on consumers’ privacy especially with different motives of the applications and service providers. Smart environment is becoming a driving factor for changing the scope and impact of the privacy protection. That is due to the fact that these technologies provide the ability to monitor and the ability to search, both are two important design privacy-related parameters[27]. General security and special privacy challenges have been identified as one of the top barriers for smart automation[28].

Generally, applications either collect data to be processed in the cloud or perform a pre-processing or a complete real-time processing[29]. However, the growing usage of the smart environment is resulting in a massive amount of data that, among other factors, makes the cloud technology an appropriate choice for computing systems. Thus the current trend is to use clouds to store and run smart environment data. Cloud technology provides wide range of services as the platform for storing collected data and running analytics related to the specific application domain. Smart environment applications can leverage the platforms and/or infrastructure services provided by clouds as storage and processing environment for the gathered heterogeneous data[30]. The main concerns and perhaps the major reasons holding off business to fully utilise clouds for personal data are security challenges and data protection concerns (including guarantees for data subjects’ rights). One major challenge for smart environment applications to utilise cloud capabilities is the user data privacy due to number of challenges and properties, as the data processing includes recognition of the activity that the user is performing, long-term behaviour patterns and personal information and health monitoring, etc…

The following subsections discuss general introduction of aspects of cloud computing and summarise the privacy principles in terms of protection goals for smart environment applications and services to be run on top of a cloud.

[25] Chapter written by Agnieszka Kitkowska, Section 4.1.4 by Harald Zwingelberg.
[26] Cook/Das 2014.
[27] Langheinrich/et al. 2004.
[28] Jacobsson/et al. 2014.
[29] Bettini/ Riboni 2015.
[30] Fazio/et al. 2015.

4.1.2 Introduction to cloud aspects

In order to define the privacy protection targets in cloud technology for smart environment services we need to understand what is cloud computing and what are the cloud services and deployment models. This subsection introduces the main aspects of the cloud for that purpose.

Cloud computing is the service of providing on-demand applications, data centres and computing resources. Cloud computing is defined in ISO/IEC 17788 [31] as: "*Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand*", where resources may include storage, software, applications, networks, operating systems and servers. The cloud provides services in three main service models: (1) Infrastructure as a Service (IaaS); where consumers are provided with controlled access to the virtual infrastructure, (2) Platform as a Service (PaaS); where consumers can deploy or acquire applications created by tools provided by the cloud provider, and (3) Software as a Service (SaaS); where consumers are using the providers application running on the cloud that is accessed via thin or thick clients[32]. Clouds could be deployed following four deployment models: public, private, hybrid and community. The public cloud is the most common deployment model in which the physical infrastructure is shared by multiple cloud clients. The architecture and infrastructure security are the responsibility of the service provider in this model. While in the private cloud, a single organization or its multiple business units use the cloud service. This type of cloud can be hosted on organization premises or somewhere else, moreover, it can be owned and managed by the cloud service provider, by the organization itself, or by both of them. Hybrid cloud and community cloud are less popular. In the community model, a specific community of clients or organizations that share some interests use the deployed cloud which could be owned by one or more of the organisations in the community. Finally, the hybrid model is the mix of two or more cloud models deployed together to enable data and application portability[33].

Although cloud computing comes with advantages in cost, resource utilisation and functionality, it is still a big concern for organisations to fully adopt their business to the cloud environment and it is hard for the users to tell whether they can trust their data and computation under the control of cloud service providers. Trust, privacy and data security are remaining challenges for adopting clouds, since data is stored in the cloud remote servers and data could be vulnerable to unprivileged access by cloud providers or even by other consumers. Though, there has not been a unified mechnisim to provide data security and privacy in cloud environment, security is managed through policy and Service Level Agreements (SLA) that is the foundation of services between consumers and providers[34] in which data privacy policies and approaches are agreed on.

In terms of data protection aspects the different models differ in particular in regard to the extent of processing of personal data that is outsourced towards the cloud provider and the level of control remaining with the controller.

4.1.3 Protection targets sorted by protection goals

Smart applications and services running in the cloud must be guaranteed basic data protection and privacy goals. For cloud users, in our case the smart environment service users, it is hard to tell whether they can trust their data and computation to be held under the control of cloud providers. Therefore, a set of security and privacy targets must be defined for analysis and considered when solutions are implemented on the cloud. The table below summarises the main protection goals and the objectives in the cloud-based smart applications based on the GDPR.

[31] ISO/IEC 17788.
[32] Zissis/ Lekkas 2012, NIST 2011; ITU-T.
[33] Alani 2016.
34 Chang/et al., 2015.

Table 3 Privacy protection goals for cloud computing for smart environment applications

Protection Goals	Objectives	Related GDPR articles
Confidentiality *data and services that process such data cannot be accessed by unauthorised entities*	- The collected data types and levels of secrecy might vary based on the exact application domain of the smart system. - Data confidentiality is required to be maintained for all the data stages during a processes life time: collection, processing usage, retention and deletion. - Data collection: communication among all components and subsystems is required to be secured. Thus only data subjects and authorized receivers can read the data. That could be achieved via applying different security mechanisms including up-to-date encryption and cryptographic systems in addition to authorization mechanisms. - Data processing: in addition to general processing environment security personal data must only be accessed by authorized processes and users and this is ensured by an access control mechanism. For this the processing operations should be defined beforehand including the entities that require access to particular personal data. Specific chare needs to be given to the decision of where and under who's control the cryptographic keys are stored to ensure effectivity of the measures taken. - Data deletion: Once the personal data is no longer necessary for the purpose pursued the data is to be deleted. Standard deletion periods should be defined and the system should support the controller with complying to this. See Art. 17 GDPR. - Data retention: Where personal data needs to be stored beyond the time necessary for the primary purpose, e.g. for specific purposes such as compliance with specific laws, such personal data has be stored securely ensuring secrecy of data via encryption and access control. However, any access to personal data by law enforcement entities requires a valid EU legal basis [35]. Controllers must ensure that law enforcement does not directly access data with the cloud provider and, where unavoidable at least provide for the ex post transparency by informing about the data breach - No own purposes of the processor: At any stage of the processing a provider of the cloud systems acting on behalf of a controller is not entitled to access the personal data for own purposes. Where possible (technical) security means excluding the cloud provider from access to the data should be implemented where possible in addition to the legal and contractual restrictions set up as part of the controller-processor relationship.	Art. 5, 25, 32

35 Art 29 WP 196, p. 5. This holds true under the GDPR as well.

Availability access to (privacy-relevant) data and to services that process such data is always granted in a comprehensible, processable, timely manner.	- In relation to the criticality level of the smart system, some minimum level of availability is required for both data and service. - Service availability: The cloud systems design ideally provides the data controller with basic services to comply with basic data subject rights, e.g. search for personal data related to a specific data subject for right of access, solutions for deletion, rectification of data and the restriction of processing. Furthermore, to maintain service availability the system requires fault detection and avoidance mechanism and a well-designed redundancy strategy – such as backups, that provides application recovery in a minimised reparation mean time. - Interoperability: A vendor-lock-in shall be avoided as this limits availability of the data and the services to the controller.[36] Difficulties for the controller to execute necessary measures including the exchange of a cloud provider should be prevented.	Art. 5 (1) (e), 13 et seq., 25
Integrity *data and services that process such data* *cannot be modified in an unauthorized or undetected manner*	- For all, collected data, data processing and stored data, content shall be proved to be not-tampered with or at least alterations must be detectable, e.g. techniques that include check-sums and hash values, etc. - Integrity mechanisms are required to be applied to all communications between components, by including proof of the data correctness among exchanged data. - To ensure integrity of data during processing, software attestation shall be achieved among remote components especially for distributed computing. - Stored data integrity: could be supported by utilising access control technical solutions and policy-enforcement for data modification. - All actions taken by the cloud provider relating to a customer's data and services should be (unchangeably) logged and transparently provided to the customer.	Art. 5 (1) (f), 25
Transparency *all privacy-relevant data processing − including the legal, technical, and organizational setting − can be understood and reconstructed at any time.*	- Data subjects in smart applications are required to realize the actual data collection process that is taking place. - Data flow and usage in addition to the data retention details has to be informed to the data subjects. That is usually referred to as: Privacy policies and announcement. As cloud systems are rather complex the declarations should be kept understandable e.g. by deploying layered policies[37] or graphic representations of data flows and entities involved. - Data subjects shall be able to realize what/how data are manipulated in the system.	Art 5 (1) (a), 13 et seq., 25, 32, 33,

36 Art 29 WP 196, p. 5.
37 Art. 29 WP 100, p 6 et seq.

	- As a matter of good practice all entities involved in the processing should be clearly named[38] so beyond the controller also the processors and sub-processors should be named including their nationality and the location of relevant computer centers involved. Controllers should be informed about the involvement of sub-processors.[39] To this end transparency and audit tools have been suggested, information about data that makes explicitly and implicitly collected and data transparent.[40] - International aspects: Where data is transferred to third countries or where based on the cloud service chosen such a transfer cannot be excluded this circumstance needs to be disclosed.	
Unlinkability privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.	- Complete unlinkability is hard to achieve due to the services that related to the subject's data, context and content in a specific domain. Thus a trade-off (threshold) should be stipulated to balance the accepted amount of linking collected data contents and the data subject. This decision should be part of the documentation available to the data subjects. - Policy implementation mechanisms are required to ensure pseudonymous and anonymous collection and processing. - The data from different cloud customers (e.g. the customers of the cloud provider be their either end users or data controllers themselves) must be clearly distinguished from data of other users by strict organisational and departmental boundaries.[41]	Art. 5 (1) (c) and (e), 17, 25
Intervenability *enforcement of the data subjects rights to access, rectification and deletion*	- Services provided as SaaS should provide for procedures to allow the fulfilment of data subjects' rights, e.g. searching for data to comply with right of access or provide data fields for blocking.[42] - At the choice of the controller the processor deletes or provides back all data to the controller, Art. 28 (3) (a) GDPR.	Art. 5 (1) (d)D and (f), 13, 14, 16 et seq. 25, 32

4.1.4 Legal considerations specific for cloud

Where cloud computing involves the engagement of one or more entities beyond the controller a controller-processor relationship is established. Thus unless in cases of pure internal usage of cloud technologies (e.g. private cloud) the requirements set forth in Art. 28 GDPR govern the relation between the controller and the processor.
For Privacy&Us specific consideration should be given to the transparency aspects. Cloud services often act worldwide to most efficiently deploy existing resources and are operated by international companies. Both facts – the processing taking place in a third country or data being processed by an entity subject to the laws of a third countries – could result to access by third parties to the data. In particular public entities may demand access for purposes such as criminal prosecution. In these

38 Art 29 WP 196, p. 6; Fischer-Hübner, Petterson, Angulo, sec. 5.1.2.
39 Art 29 WP 196, p. 6. In relation to the controller this requirement is now clearly stipulated in Art 28 (2) GDPR, demanding for a written authorisation by the controller to engage another processor.
40 Fischer-Hübner, Petterson, Angulo, sec. 5.1.2.
41 DSK, SDM, p. 29.
42 DSK, SDM, p. 29.

cases it is necessary for data controllers to be aware of such potential risks. Where applicable the fact of such transfers in third countries must be made evident to the data subjects, Articles 13 (1) (e) and 14 (1) (f) GDPR.

It is in the well understood own interest of cloud providers to present all necessary information in a transparent and intelligible way towards their customers. This includes information about processors and sub-processors,[43] data flows, location of data centres and the identity of the entities acting as cloud provider and sub-contractors.[44] It also comprises the national law(s) services provided by these entities may be subject to. This requirement is set forth in Art. 12 (1) GDPR and applies directly to cloud providers where the processing takes places in the context of an establishment in the Union. For cloud providers only established in third countries one needs to differentiate: Where services or goods are offered in the Union and end-users are their customers the GDPR applies directly to the cloud provider, Art. 3 (2) (a) GDPR.[45] In relation to businesses as cloud customers who then have end-users as their own customers the GDPR does not apply to cloud. However, the cloud user is in the role of a controller and must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures, Art. 28 (1) GDPR. The controller keeps the full responsibility for the whole processing and is advised to deliberately select the data processor. One criteria for the selection should also be the level of assistance provided by the controller to fulfil the data subject's rights, Art. 28 (3) (e) GDPR. Therefore cloud providers are well advised to proactively provide the relevant information about their services towards potential customers – and where feasible towards the pubic – as part of their market activities.
Where possible cloud providers are therefore advised to provide the necessary information in an up-to-date format, legible and easy to understand towards controllers for further distribution. At this point aspects of usability can play a role such as graphical representations of data flows.

4.1.5 Chapter summary

Processing personal data in cloud environments raises specific data protection questions which have been broadly discussed in recent years under the data protection directive. In relation to usability it can be mentioned that the GDPR sets forth clearer and to some extend stricter regime for transparency than the data protection directive. Likewise the data subject's rights to influence the processing of personal data (intervenability) need to be addressed. Both aspects are not only relevant in relation to the data subjects but also for a controller, who may herself / himself be a cloud customer but must provide all necessary information in relation its own customers. This raises questions regarding well understandable representations of the required information, ideally well usable on e.g. mobile devices.

4.2 Measuring privacy attitudes and behaviours (cloud environment)[46]

The growing number of internet users equipped in internet connected devices results in the extensive information flow between the cloud service providers (CSP) and third party applications (data controllers). Therefore, the device users (data subjects), often unaware of the service providers' privacy policies, may expose themselves to risks and harms that could result from their online behaviour. Despite of the lack of knowledge and control over the interconnected systems, people adopt the newest technologies, and use them on a daily basis. In this section, we consider the privacy protection targets and peoples' privacy attitudes and behaviours, regarding issues relevant to the cloud ecosystem of applications. We list some of the main issues relevant to the matter, emphasizing their potential influence on data subjects.

4.2.1 Introduction to privacy attitudes and behaviours

The interconnected ecosystem of cloud-based applications makes it difficult for users to understand privacy and security issues. Reports demonstrated that people express concerns about their online

[43] Bäcker in: Kühling, Buchner, Art. 13 GDPR, para. 28.
[44] Fischer-Hübner, Petterson, Angulo, sec. 5.1.2.
[45] Klar in: Kühling, Buchner, Art. 3 GDPR, para. 88.
[46] Chapter written by Lamya Abdullah, Section 4.2.3 by Harald Zwingelberg.

privacy; however, their behaviour often differs from their attitude[47]. This phenomenon, recognised in the research literature as the *privacy paradox* has been a subject of extensive studies[48].

The complex digital privacy and privacy-related decision-making process attracted the interest of investigators and researchers from various fields including law, social sciences, psychology, as well as computer sciences. The research frequently concentrates on privacy policies and visual indicators communicating information necessary for informed decision-making. Some studies demonstrated that users often disregard these indicators[49]. Among the main issues associated with reception of privacy notifications and policies, are language ambiguities[50], length[51], contextual dependencies[52], development methods[53], and display[54].

According to the GDPR, with which data processors will have to comply from May 2018, the lack of appropriate privacy and security indicators may result in legal consequences. As the new regulation guarantees data subjects' rights that they may not be aware of, it is important to improve privacy displays. The increased access to the Internet and a variety of internet-connected devices makes it cumbersome for the data subjects to comprehend what happens with their data and how the cloud applications ecosystem may affect their privacy. The unawareness of data processes and interconnectivity of applications causes potential risks, resulting in privacy harms. Therefore, a transparent representation of privacy may increase data subjects' awareness; enhance acknowledgement of harms and risks resulting from data collection, processing and dissemination.

To illustrate it better, consider the following scenario. Alice expresses general concerns about her privacy. However, she wants to improve health and lose weight, so she decides to use a smartphone fitness application, connected with a wristband and a web application. Upon sign-up, Alice is presented with two options: sign up via Social Network Services (SNS) login or create a new account. In addition, the application requires acceptance of the privacy policy and agreement to the terms and conditions (T&Cs). Upon opening the T&Cs, Alice is exposed to a long document, however, reading it collides with her primary goal – use of the new application that may improve her health. Therefore, she closes the privacy policy and decides to use the SNS login instead of creating the new account. Alice has no idea what she has agreed to. Because she did login via SNS and did not read the privacy policy, she is unaware about which data is provided by the SNS' authentication service towards the provider of the health app and which data is transferred to third countries. She is also unaware about cloud service providers (CSP) that may be involved with the processing. Alice knows nothing about the CSP and is not aware that the rights in CSP's country of origin do not comply with the EU regulations. After some time, Alice is diagnosed with a serious illness due to her overweight. As a result, Alice develops mental health issues leading to chronic depression. The doctors advise her to stop using any applications helping body weight loss, and instead focus on professional group therapy. However, despite the request for an account deletion, the personal data is being kept in multiple copies by the foreign CSP. As the CSP's encounters a security breach, Alice's data is being exposed to the public. The adversary displays her data over SNS which affects Alice's mental health by causing further anxiety or suicidal thoughts.

The above scenario demonstrates one of many possible harms resulting from privacy breaches. If Alice had been properly informed, including the engagement of the CSP in third countries where enforcement may be difficult for the controller, she might have decided differently and opted for the creation of a pseudonymous account or may have chosen an entirely different service with higher data protection standards.

4.2.2 Protection targets

To ensure an appropriate balance between attitude and behaviour of privacy related decision-making it is necessary to provide the data subjects with informative feedback. The feedback should

[47] Madden M., 2015; European Commission 2015, Eurobarometer 431.
[48] Norberg, 2007; Brown, 2001.
[49] Monteleone, Bavel, Rodríguez-Priego, & Esposito, 2015.
[50] Reidenberg et al., 2015.
[51] Bruening & Culnan, 2015.
[52] Acquisti, Brandimarte, & Loewenstein, 2015; Barkhuus, 2012.
[53] Choi & Tam, 2015; Antignac & Le Metayer, 2014.
[54] Kelley, Cesca, Bresee, & Cranor, 2010; Steinfeld, 2016; Schaub, Balebako, Durity, & Cranor, 2015.

incorporate a display of risks and harms that may result from the use of cloud-connected applications. However, the complex architecture of cloud-based applications implies constraints on the design of the suitable privacy indicators. The table below (Table 4) presents some of the protection targets, identified according to the Standard Data Protection Model (SDM) framework that may enable identification of potential harms and risks associated with privacy attitudes and behaviours in the context of cloud-based applications.

Table 4 Privacy protection goals in relation to the project "Measuring and manipulating privacy attitudes and behaviours"

Protection Goal	Objectives	Related GDPR articles
Confidentiality *data and services that process such data cannot be accessed by unauthorized entities*	**Multitenancy**: The shared environment of cloud resources puts confidentiality at risk. In order to strengthen confidentiality CSP must ensure the highest standards of encryption and key management. There are mixed views regarding encryption used in cloud services. Some recommend that data subjects should be responsible for data encryption prior to the data transfer; however, placing the responsibility of security onto inexperienced data subjects may result in overburdening them. **Outsourcing:** Appropriate access control must be implemented in cloud infrastructure. The CSPs should ensure usable and efficient authorization and authentication processes protecting data confidentiality, both for the CSP's employees, controllers and for data subjects, when necessary. The appropriate authentication should incorporate a multi factor authentication mechanism. **End-user implications**: Outsourced data is out of data subjects' control. Therefore, CSP must provide appropriate processes enabling controlled and secure retrieval of the data using secure communication channels with , e.g. transport security layer. Where the CSP is processor as an organisational measure all persons authorised to process personal data must have committed themselves to confidentiality, Art. 28 (3) (b) GDPR. Where multiple copies of data are held deletion must be processed to all instances of the dataset (see also: integrity)	Art. 5, 25, 32
Availability *access to (privacy-relevant) data and to services that process such data is always granted in a comprehensible, processable, timely manner.*	**Outsourcing**: Migrating to a cloud solution results in a loss of physical control over the organisational operations and functions. CSP should implement appropriate access control procedures to ensure rightful data access. The cloud providers' policies should be transparent, understandable and accessible by the employees at any time. **Training**: CSPs employees should be professionally trained in order to manage sensitive data. Similarly, controllers and/or data subjects should be informed by CSPs about their rights and data accessibility. **Data proliferation**:	Art. 5, Art. 15.

	The unknown number of copies of data being stored in different locations may result in an inability to provide adequate information to the data subjects, as well as controllers. This may result in false information applied in application, placing both controller and data subjects at risks, such as loss of control, reputation distortion and more. The de-duplication procedures should be in place ensuring that only accurate data is stored which enable quicker and timely access to the data **Storage limitations**: The volume of data stored in the cloud may be so high, that data deletion is necessary. CSPs must find the way to accommodate data and ensure the deletion only of data no longer required for the applications to function. An inappropriate data deletion may result in application malfunctioning, and indirectly influence data subject, for example by providing inaccurate information or application malfunction. **End-user implications**: CSPs and/or controllers have to provide an appropriate information explaining how to gain access to the personal information. CSPs must grant an access to information about the type of the data being held on their premises as well as to the data outsourced to other providers.	
Integrity *data and services that process such data cannot be modified in an unauthorized or undetected manner*	**Data provisioning**: Shared infrastructure and dynamic nature of the cloud place data integrity at risk. The widely recognized and approved encryption schemes should be applied to guarantee integrity. Clear procedures for role distribution and responsibilities among CSPs and outsourced services must be provided. **Data retention and proliferation**: CSPs must know who is authorised to delete or rectify data. Where CSP is not a controller but only a processor, the contract between processor and controller or the documented instructions should contain rules regarding the deletion of data, Art. 28 (3) (a) GDPR. The deletion of multiple data copies should not endanger integrity. Therefore, any amendments or rectifications, or deletions within the data must be implemented on all existing copies. **End-user implications**: The data subjects must be able to verify and access all their data held and stored within the cloud infrastructure.	Art. 5.
Transparency *all privacy-relevant data processing − including the legal, technical, and organizational setting − can be understood and*	**Informed consent**: CSPs must provide the user with all information necessary to understand cloud infrastructure. Where the CSP is processor on behalf of a controller the information must be provided to the controller. The consent, provided in an understandable manner, should include information about the main characteristics of the cloud, such as multitenancy, trans-border nature, outsourcing, data portability, but also other principle matters like security procedures, data subject's rights and ways to fulfil this right, as well as secondary use.	Art. 12, 13 and 14.

reconstructed at any time.	**Secondary use of data**: There must be a mutual agreement regarding the data secondary use by the CSP between the clients and the CSPs. Similarly, it is necessary for CSPs, controllers and data subjects to enter a mutual agreement regarding how and to what extent customer data is used. Therefore, an appropriate and easy access to such agreement must be guaranteed. Given the obligations of data controllers to provide transparency towards data subjects the relevant aspects of the contract between external controller and a CSP acting as processor must not be covered by confidentiality requirements and explicitly allow that the relevant information is provided to data subjects. **Informative communication**: Considering the hidden nature of data processing in the cloud, CSPs should always inform their customers (controllers or data subjects) about any changes concerning data subjects' data. The competent data protection authority and the data subject should be informed without undue delay about security or privacy breaches, such as data leakages, unauthorised secondary use of data, data outsourced to a new subcontractor etc. Where the breach is likely to result in high risks to the rights and freedoms of natural persons, these shall be informed without undue delay, Art. 34 (1) GDPR. This information must be provided to the data subject in a transparent and understandable form, according to the usability principles, guidelines and legal requirements. **User interface**: Trans-border nature of the cloud-based applications and its complex infrastructure calls for improved user interface elements explaining privacy of the cloud, such as icons or other symbols. These have to be suitable for geographic, cultural and ethnic variety of data subjects, controllers as well as cloud providers. Therefore, the user interface must be designed in such a way that it complies with usability principles (HCI guidelines as defined by Norman, Nielsen, Tognazzini and Dix [55]) and standards. The user interface should provide content accessible to all, including *"wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these".* [56] For privacy specific HCI aspects of cloud services see Fischer-Hübner et al.[57]	
Unlinkability *privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.*	**Outsourcing and multitenancy**: CSPs hosting various services have to ensure that their data is stored separately and without shared identifiers that could enable data linkability and reveal common purpose. The unlinkability must be ensured to protect from risks, such as profiling, identification and more Multitenancy in cloud computing raises issues of the level of data separation between the tenants that should be addressed by CSPs. **Isolation**: Data should be completely isolated through the entire lifecycle in	Art. 5, 15 and 21.

[55] Norman 2013; Nielsen 1994; Tognazzini 1993; Dix, Finlay, Abowd & Beale 2010.
[56] WCAG 2.0 Guidelines for web content accessibility, https://www.w3.org/TR/WCAG20/
[57] Fischer-Hübner, Petterson, Angulo, sec. 5.

	order for the controller/data subject to be protected. The specific threats should be protected with appropriate encryption methods applicable to the cloud service (PaaS or SaaS) in question. Where encryption is used as a solution key handling must be clearly defined. Ideally, keys are handled by the entity responsible for the data processed. **Data Minimization**: CSPs should only store data necessary for the appropriate functioning of applications. A limited amount of collected data decreases the risk of linkability. In particular the necessity of the storage of metadata such as log-files needs to be minimized. **Encryption**: Ensuring unlinkability of pieces of information distributed over cloud by maintaining the keys, for example by using secure pseudorandom number generators etc. **Access control**: CSPs should ensure that personal data access is granted in a way that eliminates a risk of data linkability, by an appropriate distribution of roles and rights, authentication and authorization, and set of suitable policies and regulations internal to CSPs. **Data deletion**: Upon the data subjects' request, the data should be completely deleted. However, due to data duplication, it is sometimes impossible to ensure that all data is removed. The CSPs should use client-side cryptography to ensure that once the data subject destroys the keys necessary to decrypt data blocks, these blocks become inaccessible. This improved security measure, if sufficiently explained, may help data subject to understand the minimised risks such as identification or unauthorised access. .	
Intervenability ***intervention is possible concerning all ongoing or planned privacy-relevant data processing***	**Accessibility**: Outsourced data is out of data subjects' control. Therefore, CSP or controller must provide appropriate tools enabling control retrieval. CSPs therefore should ensure an easy access to the processed data, allowing for amendments or deletion. **Data portability and provider lock-in:** The data subject has a right to withdraw consent and requests the data to be provided to the data subject in a format appropriate for the data transfer to other CSP. The portability property aims to achieve data transferability, among different cloud providers and services. Data or vendor lock-in could result in a lack of data portability and interoperability between different cloud services. The use of a non-standard format could impose obstacles in the transfer of personal data or result in data disuse, due to the lack of compatibility, for example in a case of data vendor bankruptcy. **End-user implications**: Data subjects should be able to access and process their data regardless of the cloud service's architecture. A cloud vendor may rely on other provider's (subcontractor) services in order to offer his services. That should not be an obstacle for the data subject to intervene to his data, in fact, the cloud vendor must be able to provide all the technical and organisational means to achieve this goal.	Art. 15, 16, 17, 18, 19 and 20.

	Data subjects must be able to access, delete, amend, and restrict access to their data at any time and through any means. **Trans-border nature of the cloud:** Where data is shifted within bigger cloud structures into computer centers outside of the territorial scope of the GDPR controllers must be informed beforehand and given opportunity to intervene, Art. 28 (3) (a) GDPR.	

4.2.3 Legal considerations

From a legal perspective the user's attitude and behaviour may be of secondary importance. While studies may show that many persons appear disinterested in how, where and by whom their personal data is processed, the legal requirements provide a clear setting. Here Art. 12 et seq. GDPR demand transparency and detailed information to be provided in an understandable manner and complete enough so that data subjects can make an informed decision. While a more interested attitude may of data subjects may be preferable the law is not oriented at the average data subject but for the protection of basic rights must have the person in mind that wants to get insight in what happens with her or his personal data. Regarding legal considerations on transparency requirements, we like to refer to the aspects set forth above (section 4.1.4).

In legal practice we are likely to encounter difficult to describe and understand multi-party relationships where all parties pursue own purposes, e.g. a service provider with the service for the end user, an entity providing targeted advertisement and the CSPs as entity running the backend systems with own secondary uses for the data obtained. While it is already challenging to disentangle such constructions for a sufficiently precise description for documentation purposes the legal assessment and classification between controllers, processors or joint controllers will cause problems and force the parties to describe their business models and purposes pursued in detail. This has particular consequence for the internal liability between parties, cf. Art. 82 (2) GDPR. In relation to the end users both – lawyers and HCI-experts – are challenged to develop understandable descriptions of the processes involved. This also includes new ways to display such information e.g. by virtue of specific icons, see Art. 12 (7) GDPR.

4.2.4 Chapter summary

This chapter aimed to present main privacy targets related to the users' privacy decision-making in the ecosystem of cloud-based applications. The primary goal of this chapter was to identify privacy targets that will contribute to privacy risk assessment for cloud-environment. Additionally, the identification of privacy targets should benefit developers and designers of cloud-based applications, as well as CSPs, to ensure the compliance with the GDPR. On the other hand, a greater understanding of risks and harms will enable informative feedback provided to the end-users, which should result in diminishing the gap between privacy attitudes and behaviours.

4.3 Privacy indicators in Smartphone Ecosystems[58]

4.3.1 Introduction to Smartphone Ecosystems

With the growing proliferation of smartphone applications (apps), smartphone ecosystems are envisaged to provide a remarkable value to businesses (service providers) and to society as a whole. The term 'smartphone ecosystem' comprises smartphones' hardware and software platform including apps running on top of the platform, as well the infrastructural components such as app markets (e.g. Google Play, App Store). In principle, three entities namely, users, app developers and app stores

[58] Chapter written by Majid Hatamian, Section 4.3.3 by Harald Zwingelberg.

play an important role in smartphone ecosystems[59]:

- Users of apps, which are directly or indirectly benefiting from app stores by downloading and using their desired apps.
- App developers, which are involved in the mass market (app stores) of apps by developing apps for smartphones, mobile devices, etc.
- App Stores, which are rich sources of apps and serve as a communication interface to directly or indirectly communicate with application developers and users.

While smartphone apps provide tremendous benefits to users, especially in terms of personalized and context-sensitive services; having access to a multiplicity of sensitive resources also poses a series of privacy risks such as user profiling, tracking and identity theft. Furthermore, many apps access resources which are not even required to provide the needed functionality to users, instead, they do so, either to support the business models of service providers (e.g., targeted advertising), or just because of the lack of a privacy preserving culture (knowledge) among app developers[60]. While hungry permission apps already pose several privacy risks to users, the more critical issue arises from the users' unawareness with regard to the data collected by their apps. Accordingly, users continuously and increasingly express discomfort once they realise that their data are being collected without their informed consent.

In the light of the recently approved GDPR of the EU, which is assumed to regulate the provision of a stronger control of personal data to individuals; an important challenge is the implementation and enforcement of the "data protection design" principle in Art. 25 (1) GDPR. This principle emphasizes how critical the implementation of transparency and informed consent is; it makes the need for providing measures explicit that enable users to better understand the privacy risks resulting from the processes of data sharing. In this regard, smartphone ecosystems are challenging because of the privacy issues resulting from the extensive use of personal data by smartphone apps. Additionally, the openness of certain operating systems and the lack of reliable permission information enable app developers to request unnecessary permissions, mostly resulting in over-privileged apps. In the following section we elaborate more on the specific challenges and protection goals in the smartphone ecosystems area.

4.3.2 Protection targets sorted by protection goals

This section introduces a set of privacy relevant challenges in smartphone ecosystems; followed by the identified privacy protection goals and operational requirements.
In general, the main challenge in the smartphone ecosystems is the lack of transparency in regard to the data that are being accessed by smartphone applications. More precisely, current models do not make evident to users by whom and to which extent (including number of occurrences) these data are collected, transferred and processed. This important issue could be addressed by providing the tools for users to understand which data is being accessed by which app, and for which purpose. Furthermore, the lack of privacy risk information regarding the resources accessed by mobile apps makes it difficult for users to determine whether to install the app or not; users do not understand the implication and consequences of sharing different types of data. Accordingly, they feel disappointed once they realise that their data are being accessed without being provided by a transparent and understandable privacy indicator. As the aim of this project is mainly to provide suitable privacy indicators, we propose a tool that will address the following concrete challenges in the smartphone ecosystems.

[59] Wei, X. (2013). Understanding and improving the smartphone ecosystem: measurements, security and tools.
[60] Nauman, M., Khan, S., and Zhang, X. (2014). Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help?

Table 5 Privacy protection goals for smartphone ecosystems

Challenge	Informed Privacy Decision (transparency)
Objective	Any installed app that uses, collects, transfers, and processes personal information must prepare adequate, appropriate, and efficient mechanisms by which the user will be able to make informed privacy decisions.
Motivation	Current smartphone apps are missing the capability which allows users to make informed privacy decisions. That is why once users figure out that they are not able to make informed decisions regarding their privacy, they express discomfort.
Requirements	It is necessary to implement usable, appropriate and efficient privacy indicators in the form of Graphical User Interface (GUI) by which we support and enable users to make informed decision regarding their privacy. Solutions should embed psychological aspects of privacy while designing the GUI which further ameliorates informed decision making.

Challenge	User-centric (transparency, intervenability)
Objective	User-centric privacy preservation must be taken into consideration in planning und operating phases (privacy by design, Art. 25 (1) GDPR). As a result, a privacy preservation approach regarding the user's needs for information and possibilities of interaction is proposed.
Motivation	Many of the existing solutions for assessing privacy risks in smartphone ecosystems do not consider a user-based privacy preservation approach. In fact, they are suffering from a lack of user input. For this reason, we should not neglect analysing privacy according to the value of each smartphone sub-asset (e.g. contact list, usage history)
Requirements	There is a need for tools that provide information regarding sensitive data access from smartphone apps and tools to report privacy aggressive behaviour of applications. This should be done by mechanisms to analyse and monitor access to permissions according to the usage patterns. Mechanisms to properly inform the user about the results of the analysis, including understandable privacy indicators. Mechanisms that enable users to report or provide feedback regarding their perceptions about the invasiveness level of an app. Providing users with transparency and possibilities to interact by granting or revoking rights for apps (intervenability) must not, however, lead to a situation where the programmers' and data controllers' responsibilities are transferred to the users. In addition the default settings must be privacy preserving, (privacy by default, Art. 25 (2) GDPR).

Challenge	Privacy Preservation before Installing Apps (transparency)
Objective	The user should be able to understand in a clear and concise manner the privacy invasiveness level of apps before installing them. This functionality will support them to make informed decisions before app installation and potentially be able to install a less privacy aggressive app.
Motivation	This fact lies down on this principle that every privacy invasive activity should be anticipated and prevented before happening. As a result, assessing privacy invasiveness level of apps before installation (e.g. by getting help from crowdsourcing) will considerably help users to compare apps in terms of privacy invasion.
Requirements	We require mechanisms and tools to evaluate the privacy level offered by apps in regard to the permissions needed. In fact, tools should provide a clear view and understanding of which apps are over-privileged apps.

Challenge	Privacy Preservation after Installing Apps (intervenability)
Objective	The user should not be required to do any further efforts which entails specific knowledge about privacy preservation after installing apps. Users with any level of knowledge, age, education, etc. should be able to easily control, handle, and manage their privacy after installing apps.
Motivation	This fact lies down on this principle that the app developers must not forget and neglect the right of the users for preserving their own privacy after installing apps. This is due to the fact that, after installing apps, users admit and grant all the permissions needed for the functionality of a given app. As a result, they must have this right to control their privacy after installation.
Requirements	First, tools that track the permission usage and inform users about the behaviour of the installed applications should exist. Second, mechanisms that enable users to restrict/grant permissions to access their data should also be available.

In the following we identify the main protection goals related to the identified challenges:

Principle	Confidentiality
Description	Personal data must be protected from unauthorized access.
Motivation	Users should be assured that intruders do not have access to their personal data.
Operational Requirements	Data collected and processed by the smartphone or data collectors (i.e. service providers through smartphone applications) must be securely stored and, if applicable, securely transmitted. This is done by implementing appropriate security mechanisms at the communication/transmission level and at the storage and data access levels: - End-to-end encryption - SSL transmission - Access control at the user and server side

Principle	Integrity
Description	Personal data must be protected against unauthorised or unlawful manipulation.
Motivation	Users should be assured that intruders cannot manipulate their personal data.
Operational Requirements	Information collected from the user device and transmitted to the service provider should remain authentic and be protected from manipulation. This is done by implementing security mechanisms such as digital signatures.

Principle	Intervenability
Description	The users should have the right to rectify, block, or erase their data.
Motivation	Users should be given with the assurance that the data controller provides them with appropriate mechanisms to have control over their data.
Operational Requirements	In the design of the proposed artefacts, users will be provided with privacy indicators regarding the right to notification, information, rectification, blocking and erasure at any time. We will support, manage, and handle all collected personal data in a privacy and security friendly fashion. Where data is shared or transferred to third parties by the programmer, shop or other entity this must be made transparent and the user needs an option to control this behaviour unless the transfer is necessary to provide the desired service.

Principle	Availability
Description	All the personal data shall be available as long as the purpose of collection, transmission, and processing is still valid.
Motivation	The users should have access to services and data provided and used by smartphone applications in a timely manner.
Operational Requirements	Optimising approaches might be needed to decrease the time of processing data to make accesses to privacy relevant data as quick as possible. The required degree of availability highly depends on the importance of the service provided by the app, e.g. health apps may have a higher need than online games.

Principle	Transparency
Description	Any installed app that uses, collects, transmits, and processes personal information must provide an acceptable level of transparency for the users. This will enable users to understand why, by whom, and to which extent their data are being accessed, collected, transferred, and processed.
Motivation	As a result, when an app does not provide transparency, the user will not be able to sufficiently understand the implications and consequences of her decisions regarding privacy
Operational Requirements	In smartphone ecosystems, users should be **informed** about permissions and data being accessed, transmitted and processed by apps. A **data track** module could interactively inform users about the flow of their data (including frequency of accesses). Users should be provided with effective **privacy indicators** that show in an understandable way how privacy friendly or invasive an application is. Where data is shared or transferred to third parties by the programmer, shop or other entity this must be made transparent and the user needs an option to control this behaviour unless the transfer is necessary to provide the desired service.

Principle	Unlinkability
Description	The users should be able to perform multiple actions without others being able to link these actions together. Where possible also the app provider and the entity running a necessary backend should be unable to link users' activities.
Motivation	Users should have the possibility to, e.g., make their activities private while using smartphone applications.
Operational Requirements	A mechanism that enables users to selectively grant access to their data and to select which data/activities should not be linked by smartphone apps, programmers and providers of backends.

Principle	Data Minimisation
Description	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Motivation	Users must have the possibility to, e.g., authenticate to services with only those attributes of a credential essentially required for authentication. Smartphone applications should collect only information relevant to provide described

	functionality and potentially that to support the business model.
Operational Requirements	Users should have the possibility to select which information are collected and transmitted to services providers by smartphone apps. Ideally, only the necessary amount of data should leave the device and when services do not require data such as users' ID, phone number, should not be collected.

4.3.3 Legal considerations in smartphone ecosystems

In the field of smartphone apps, mobile communications and online services the upcoming ePrivacy regulation[61] will supersede the GDPR where applicable. At the time of editorial deadline for this document the Regulation on Privacy and Electronic Communications (ePrivacy Regulation) was still under discussion within the European Parliament and a final text is not available. Based on the available drafts some first insights relevant for users, app-programmers and other involved entities include:

- The first drafts have a clear tendency to move away[62] from the GDPR's principles of data protection by design and by default and to shift responsibilities away from the controllers towards the users. This becomes evident by a comparison of the internal draft from December 2016[63] and the published in February 2017:

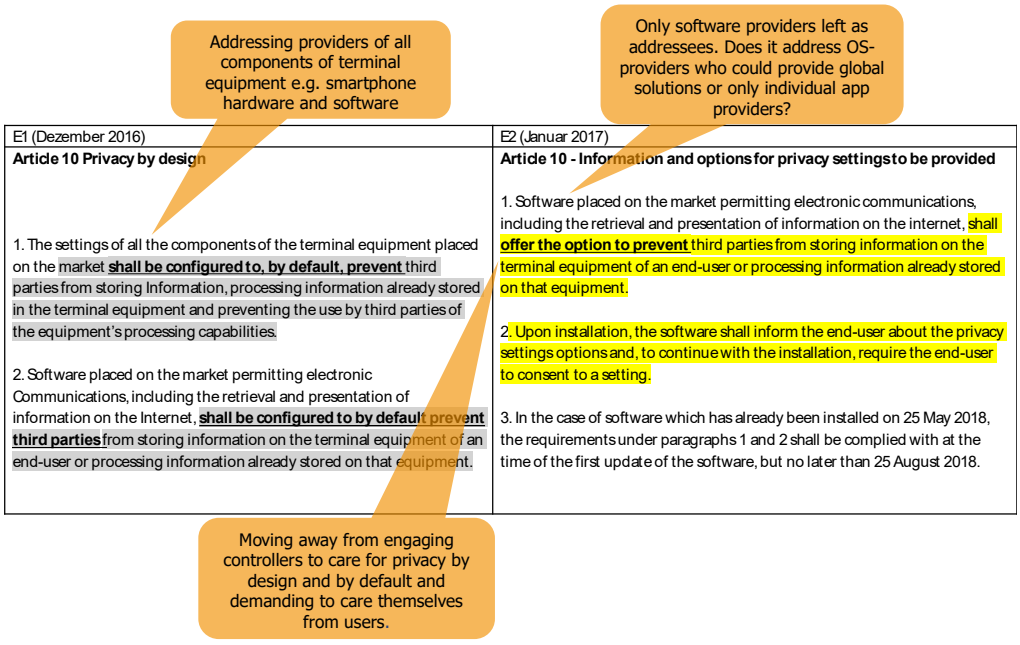

Figure 2 Art. 10 ePrivacyReg draft version of Dec. 16 vis-a-vis Feb. 17[64]

- Generally from a privacy position a return to the December version is preferable bringing the generic principles of privacy by design and privacy by default set forth in Art. 25 GDPR to the specific ruleset in the ePrivacy Regulation. This is strongly supported by the Art. 29

[61] Considerations are based on the draft published in February: 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), online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010.
[62] Art. 29 WP 247 para 19; Zuiderveen et al. p. 93 et seq.
[63] Source for the leaked version of the December draft: http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf
[64] Based on slide set by Zwingelberg, online: https://www.datenschutzzentrum.de/uploads/2017-03-10_GI-Workshop_PET-und-DSGVO_Zwingelberg.pdf

Working Party,[65] the European Data Protection Supervisor[66] and a study[67] prepared for the LIBE committee of the European Parliament. From a usability perspective it would be highly desirable to have at least mandatory requirements regarding the ease of use. This could include:

- develop or offer UI solutions with a minimal effort for navigation and learning by the user. In the context of choosing data protection settings ideas for concrete solutions that might be considered could be:
  - a one-click solution to obtain the settings that should have been provided as privacy by default in the first place,
  - easy slider-type selections between different levels to select between privacy and additional functionalities and
- the provision of expert modes to fine granularly choose options.

- - To this end a first draft report LIEBE rapporteur, MEP Marju Lauristin, suggests a shift back towards keeping the privacy considerations of the GDPR by changing art 10 paragraph 1 and paragraph 1a of the ePrivacy Regulation to read as follows:[68]

> "(a*) by default, offer privacy protective settings to prevent other parties from storing information on the terminal equipment of a user and from processing information already stored on that equipment;*
> *(b) upon installation, inform and offer the user the possibility to change or confirm the privacy settings options defined in point (a) by requiring the user's consent to a setting;*
> *(c) make the setting defined in points (a) and (b) easily accessible during the use of the software; and*
> *(d) offer the user the possibility to express specific consent through the settings after the installation of the software.*
>
> *1a. For the purpose of points (a) and (b) of paragraph 1, the settings shall include a signal which is sent to the other parties to inform them about the user's privacy settings. These settings shall be binding on, and enforceable against, any other party."*

This quick introduction can only accomplish to selectively point to aspects of the ePrivacy Regulation central to privacy for smartphone apps with close relation to HCI-considerations. However, as aspects of usability are directly part of the proposed wording of the regulation it also shows the relevance given to these topics. As observed under the discussion of the GDPR in the parliamentary process and the following trilog we are to expect influences of lobbying groups and several changes and amendments of the proposed text. Once a final text is available – planned for May 2018 – the relevance for the further research in this field done as part of Privacy&Us needs to be reflected further.

Besides the ePrivacy Regulation specific considerations some more generic legal considerations on the topic of privacy in smartphone apps include:

- Technical security measures were listed in order to protect confidentiality. Also, in this case, it is necessary that the multiple service providers that interact in the mobile context have contractual and organizational safeguards to protect confidentiality.
- Art. 15 GDPR provides the right of access to personal data processed by a controller. With smartphones data processing and storage may happen on the device. Where data is stored locally on a smartphone device and not under the control of a backend device this personal data may nevertheless be under the responsibility of the app- or service provider as controller. Following the underlying thought of Art. 11 and recital 64 GDPR the

[65] Art. 29 WP 247 para. 19.
[66] EDPS 6/2017 p. 18 et seq.
[67] Zuiderveen et al. p. 93 et seq
[68] Lauristin, amendments 94 et seq.

controller should not be forced to first collect the data to then provide the user with the information. Rather it may be preferable to provide the user with functionalities to view (right of access) and export (right to have a copy, Art. 15 (3) GDPR).

- Security measures that should be taken in order to avoid unlawful or unauthorized manipulation were mentioned. On this issue, also organizational and contractual measures shall be undertaken, both within the organisation and between the third-parties that will have authorized access to the data
- Transparency and consent might also be a challenge, as many apps are constantly collecting data. It is still uncertain how frequent and how detailed should the notifications be in order to: a) properly inform data subjects about data collection and processing; b) do not interfere with the usability. There is also the challenge of what data, when and how to convey to data subjects.
- Unlinkability might be a difficult principle to implement in smartphone environments, given that in many apps the data are stored in the device and the data subject does not alter the default of the device to a more privacy preserving option. The consequence is that the device data is shared among apps, sometimes without the awareness of the user, harming both unlinkability and transparency. Here Art. 10 ePrivacy Regulation could provide a remedy, if hardware producers and OS providers are forced deliver products with privacy preserving default settings.

4.3.4 Chapter summary

In this chapter, we clarified the privacy protection targets essential for smartphone ecosystems. We first introduced challenges induced from the smartphone apps. These challenges will further enable us to better realise the main privacy targets sorted by protection goal. Consequently, we introduced the main protection goals related to the identified challenges. This section follows by legal considerations in smartphone ecosystems that are aimed to consider legal principles crucial regarding embedding privacy targets in the core of the proposed artefacts. As the ePrivacy Regulation is still in the parliamentary process a final legal evaluation based on the final text is pending. Of crucial relevance to smartphone ecosystems will be the controversially discussed article 10 of the draft ePrivacy Regulation.

4.4 IoT and smart spaces[69]

The Internet of Things (IoT) can be defined as *"a set of devices, sensors or actuators – that connect, communicate or transmit information with or between each other through the Internet"*[70]. We define "smart space" as a space equipped with IoT technology.

IoT is going through a rapid expansion phase, this is seen in metrics such as the number of connected devices per person (Globalwebindex, 2016), the number of published papers on this subject (Mendez, Papapanagiotou, & Yang, 2017), or the number of IoT projects supported by the "do it yourself" community[71]. Some major industry players have committed to expanding their presence on the IoT market, a notable example is Samsung's[72] goal to make all of their devices IoT-enabled by 2020.

Such a growth can bring important technological and economic benefits to humanity, in terms of energy efficiency, health improvements and other aspects that affect the quality of life. However, it also comes with privacy-related implications, which will become major issues if not handled at the right time.

The complexity of IoT privacy is rooted in multiple factors, such as the novelty of the concept and the lack of awareness of how the technology works, poor usability and resource-constrained hardware. The effect is exacerbated by the fact that IoT devices are typically installed in very exclusive locations – in a person's home or on their body, which guarantees unfettered access to very personal information. Another key ingredient is the availability of enormous quantities of data that can be

[69] Chapter written by Alexandr Railean.
[70] Adapted from (FTC, 2015)
[71] As of this writing, there are 21714 projects on github.com and 34000 projects on instructables.com matching the `iot` tag
[72] http://mashable.com/2015/01/05/samsung-internet-of-things

analysed and correlated; further, there are techniques that can deanonymise a data subject even after data minimization measures were taken beforehand.
For example, imagine a hypothetical scenario in which a neighbourhood uses smart meters to minimise energy use by collecting and publishing power consumption metrics for each household in the area. A benefit is that every family has better awareness of their energy footprint and thus strives to use fewer resources and save money; there is also a gamification element involved – can our family become "the greenest household in the neighbourhood"? Can we "beat" our next-door neighbour? Can we use less energy than we used this month last year? On the other hand, burglars benefit from such information as well – they know the hours when a house is most likely to be empty, they can also infer that the house with the greatest energy consumption belongs to the richest family – making them an attractive target. Another possibility would be observing that a particular house appears to be most active at night – this could mean that the person who lives there has a sleeping disorder, which in turn reveals details about their health or behaviour that they would rather keep to themselves. To make matters even more complicated, imagine that the data are also analysed by some companies who then use the information to aggressively market their products to specific households, or sell the data to insurance organizations, empowering them to charge higher rates when they can get away with it.
Would the family that has "the greenest household in the neighbourhood" decide to participate in the IoT experiment if they were aware of these unforeseen side-effects?
Due to the great diversity of sensors, and the continuous shrinking of device sizes as a result of technological progress, it is difficult to imagine a scenario in which IoT cannot be applied, and it is difficult to anticipate the ways in which this technology can be used against an individual's best interests.

The rest of this chapter examines the concept of IoT from the perspective of protection targets, as defined by the General Data Protection Regulation (GDPR).

Table 6 Privacy protection targets for IoT and smart spaces

	IoT and smart spaces	Related GDPR articles
Confidentiality *Data and services that process such data cannot be accessed by unauthorized entities*	***Encryption vs resource constraints*** - some IoT technology consists of minimalistic, ultra-low-power devices, which may not have enough capabilities to implement adequate, in-place data-encryption techniques to protect data at rest and in transit. This can expose IoT devices to man-in-the-middle attacks or eavesdropping, giving an adversary the chance to access the data or manipulate them before they reach the destination. Other consequences could be the ability to spoof commands sent to an IoT device (e.g. to open a door by impersonating the real data subject) or plant evidence that will incriminate the data subject (e.g. send a fake location tag that puts them at the scene of a crime at a specific time). ***Cloud-based storage implications*** apply if IoT devices rely on remote servers for data storage (see chapter 4.1.3 for a detailed review).	Art. 5, 25, 32
Integrity *Data and services that process such data cannot be modified in an unauthorized or undetected manner*	***Data manipulation*** can occur while information is transmitted or stored, unless specific actions were taken to protect against that. A variety of cryptographic primitives can be applied to ensure that the data are not altered, e.g.: hash functions, digital signatures, authenticated encryption or message authentication codes (MAC). For contexts where remote servers are involved, please refer to chapter 4.1.3 for an overview of other integrity protection measures.	Art. 5.

Availability *Access to (privacy-relevant) data and to services that process such data is always granted in a comprehensible, processable, timely manner*	***Vendor lock-in*** through the use of proprietary software exposes data subjects to the risk of losing the ability to use the data if the vendor goes bankrupt, decides to discontinue the service or makes it unjustifiably expensive. Art. 20 of the GDPR stipulates that data subjects have the right to export their data for use in services managed by other data controllers; however, this provision can be circumvented through the use of convoluted formats that hinder interoperability. Therefore it is important to encourage the use of open standards and make this information easily available to potential data subjects before they start using a specific IoT device or service. ***Maintenance barriers*** (e.g. non-removable batteries, "tivoization"[73]) can be imposed to prevent data subjects from using their IoT devices or updating the software after the manufacturer discontinues it. Additional legislation that protects a data subject's right to repair[74] will reduce such barriers. ***Denial of service*** attacks launched by third parties (e.g. state actors or criminal organizations) can jeopardize data availability, even if there is no ill will on the side of the data processor or the data controller. This can have critical consequences if any health-care related services rely on the targeted IoT infrastructure ***Scalability*** constraints arise when dealing with a smart space located in a public area. Assuming that the space provides an interface data subjects can interact with – how many people can it serve at once?	Art. 20, 13
Transparency *all privacy-relevant data processing – including the legal, technical, and organizational setting – can be understood and reconstructed at any time.*	***Lack of a user interface*** – some IoT products are small, low-power devices that have no displays that can explain to a data-subject what the device is doing. This offsets the burden of transparency-compliance onto something else (e.g. product box, user's guide or manufacturer's web-site, accompanying smartphone application, etc.) and cannot be resolved by means of usability improvements of the device itself. ***Consent*** – the aforementioned lack of an interface implies that the device requires external means of requesting informed consent, as well as allowing the data subject to withdraw it later, in an easy manner. An alternative way would be to give or withdraw consent by contacting the data controller using other channels (e.g. phone or email), which requires contact information to be easily accessible, as stated in Art. 13. ***"Invisible" IoT devices*** that are embedded into an environment, thus turning it into a smart space, pose an additional challenge – people may be unaware of the fact that they are in such a space, hence not even realize that they need to decide whether they provide consent or not. Therefore it is important to establish a system of signs that can be relied upon when navigating an area. ***Interface complexity*** can lead to a poor understanding of how an IoT device operates, as such – data subjects will not be able to make informed decisions. Therefore user interfaces should be designed while considering the best practices of usability research. Art. 12 (7) suggests the use of standardised (machine-readable, when appropriate) icons to meet this requirement.	Art. 7, 12, 13

[73] Applying cryptographic digital signatures to prevent the use of alternative software or firmware.
[74] European Parliament, Motion for a Resolution on longer lifetime for products, see sections 9 et. seq., online: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0214+0+DOC+XML+V0//EN

	Deceiving interfaces can be the result of a compromised IoT device that was reprogrammed to change its behaviour with respect to transparency. For instance, a hacked camera can change the interface in such a way that the LED that indicates that the camera is recording will be off all the time, regardless of the camera's state. This is a security issue related to the integrity of the equipment itself, but it can also be addressed by employing specific industrial design practices, such as adding mechanical switches that make it clear that a sensor is unpowered and physically unable to acquire any data. **C*onflicting choices*** each data subject has their own preferences regarding the behaviour of a smart space; how shall the space behave when people with conflicting preferences are located in it? For example, a camera cannot "record" and "not record" at the same time, how can it reconcile the mutually contradicting wishes? This is a technical challenge that has to be addressed in order to ensure that the provisions of the GDPR are respected.	
Unlinkability *privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.*	***Quantity becomes quality*** – when large sets of data are available for analysis, one could reveal patterns related to the behaviour of a data subject. There are several possibilities: • *One set*: we can exemplify this by referring to a log of anonymized search queries published by AOL in 2006. The database was shared for research purposes, but was accessible to the entire world. The information spanned across a period of 3 months and contained twenty million search keywords, and it facilitated the identification of individual users (e.g. by examining the keywords they searched for, which could contain their own name, address, nearby businesses, etc.). This can be prevented by applying the k-anonymity[75] model before releasing the data. • *Multiple sets*: a relevant example is the Netflix dataset, which contained anonymized records of movie-preferences of Netflix users. The data from the set was correlated with publically available details on another web-site, IMDB; this was sufficient to successfully identify users[76]. While the law obliges the data controller to use the data only for a specific purpose, it cannot control what happens if they get hacked and an unauthorized party obtains the data (besides reporting the incident, as dictated by Art. 33 GDPR). Thus, the challenge for unlinkability is to anticipate what new knowledge can be obtained by someone with access to vast data sets. Some basic measures towards this end are stated in Art. 5 GDPR, e.g: data minimisation, time-limited storage. The corresponding systems should be engineered such that they do not reuse the same identifier for a data subject in different data sets. ***Cloud-based storage implications*** apply here as well (see chapter 4.1.3 for a detailed review).	Art. 5, 14
Intervenability *intervention is*	***Lack of an interface*** – an IoT device may sometimes lack the means to display, edit or delete the data collected. This is also relevant in cases where limited storage capacities are available on the device	Art. 7, 13, 16, 17

[75] K-anonymity, a model for protecting privacy, Latanya Sweeney, 2002
[76] Robust de-anonymization of large sparse datasets, Narayanan, Shmatikov, 2008

possible concerning all ongoing or planned privacy-relevant data processing	itself, implying that other data are located elsewhere (e.g. on a cloud-based service). This means that data-subjects cannot easily exercise their right to intervene, without resorting to other technology, such as a web-browser or a smartphone application (which can be a problem if the data subject does not own a smartphone, a tablet or a computer). In any case the data controller must provide a process in case a data subjects asks for access, rectification or deletion. ***Shoulder surfing*** is another issue that arises during public use, as passers-by can get a glimpse of another subject's personal data or preferences. Therefore smart spaces should provide interfaces that allow viewing or editing data in a private setting (e.g. through a data subject's own smartphone) ***Minors are a special case*** – according to recital 38 of the GDPR, children merit specific protection under the regulation. As such, an IoT device or a smart space may be in the need to determine the age of the data subject, in order to decide whether their consent is sufficient or not. However, this requires processing of personal data, e.g. a picture of the face. Special measures have to be applied, to ensure that only the bare minimum of information is supplied; for example a filtering algorithm[77] implemented in a trusted hardware component can pre-process the data before it reaches the IoT device in a smart space.	

4.4.1 Legal considerations in IoT and smart spaces

From a legal perspective, IoT and smart spaces have common themes with other sections discussed in the document. In cases where cloud-based solutions are involved, arguments listed in section 4.1.4 apply; please refer to the notes regarding the controller-processor relationship and the situations in which data are stored abroad.
The transparency-focused legal analysis in section 4.2.3 applies here as well, as data subjects need to be aware of how their data are handled; please refer to the notes suggesting how this can be accomplished (e.g. the involvement of HCI expertise, icons, etc.). However, with smart spaces, the factual possibilities to provide the necessary information are highly limited, as many devices do not have displays or other means to easily communicate the information that must be provided according to Art. 12 et seq. GDPR. With many devices being tiny, the packaging does not provide a sufficient solution.

A unique aspect that relates to smart spaces deployed in public areas is the fact that they may have to deal with a great flow of pedestrians passing through it. If any personal information is recorded (e.g. video footage or static shots that may reveal a person's face), the organization that manages the smart space will fail to comply with Art. 14 of the GDPR (individually notifying the data subjects). Where the identity of the data subjects is not known to the controller, Art. 10 GDPR applies, and it is not necessary and not permitted to identify the data subjects for the sole purpose of notification. Rather, a public communication of the data breach is necessary, Art. 34 (3) (c) GDPR. In any case, controllers responsible for smart spaces are highly advised to have measures in place that provide sufficient protection of the personal data, such that these are unintelligible to any third party e.g. by use of encryption, Art. 34 (1) (a) GDPR. This is usually sufficient to protect data subjects from high risks of exposure However, see section 4.5.3 for genetic data, which argues that in specific circumstances, this may still pose a high risk for data subjects as it may still affect their relatives for a long timeframe.

The dynamic nature of such interactions (e.g. cycling through a smart space at high speed, or merely walking at an accelerated pace) raises the question of the lawfulness of the processing. Requesting consent may be highly impractical. Therefore one of the other legal grounds enumerated in Art. 6. (1)

[77] Jana et al, 2013, A Scanner Darkly: Protecting User Privacy From Perceptual Applications

GDPR must be given to process such data. However, in case of Art. 6 (1) (e) and (f) GDPR the controller must conform to Art. 21 GDPR, providing the data subject a right to object. Besides having a process in place to comply with such a request, the data subject also needs to be sufficiently informed as to where and how this right can be exercised. We believe that an adequate way to handle this is by placing an emphasis on transparency, e.g. through the use of icons that would mark a smart space accordingly, giving data subjects a choice to simply not enter the space before data are collected. Likewise, the identity and contact details of the controller must be clearly specified. One possibility to accomplish this is via QR-codes with the necessary information and potentially, the means to communicate an automated request for an objection.

Another unique characteristic of smart spaces is related to the scale of interaction – if there are hundreds of people in the central square of a city, which happens to be a smart space, how do we ensure the transparency requirements and implement Art. 16 (right to rectification)? Addressing this concern requires new ways of interaction.

4.4.2 Chapter summary

This chapter introduces the main challenges posed by IoT and smart spaces, and identifies the privacy-related issues that arise throughout the use of such technologies. Further, it maps each of the protection targets to problems that are specific to IoT and smart spaces, and references the corresponding GDPR articles. In addition to that, we have suggested solutions, derived from the relevant research literature.

4.5 Genomic Privacy[78]

4.5.1 Introduction to Genomic Privacy

We are experiencing the transition from traditional medicine to personalized medicine and its newer counterpart, precision medicine[79]. This promising new way of medicine allows physicians to assess better the disease susceptibility of their patients, understand better how these diseases will affect them and allows the physicians to evaluate the optimal therapy for each patient.

Unsurprisingly, this revolutionary approach was quickly embraced by the private sector. In 2006, a company called 23andMe was founded offering direct-to-consumer (DTC) genetic testing and providing ancestry and health genotyping to its consumers. Shortly after, dozens of similar companies surfaced all around the world, providing similar or more specialized services.

This tendency affected governments as well and as a result, in the last five years we witnessed the birth of various governmental genomic projects. These projects aim to build biorepositories containing the sequenced genomes of hundreds of thousands of patients in the hopes of providing better healthcare for their patients. Genomics England, an Department of Health project funded by the UK government, aims to sequence 100,000 genomes of NHS patients by the year 2017 in order to "enable new scientific discovery and medical insights"[80]. However, by June 2017, only 31,730 had been sequenced. On the other side of the Atlantic Ocean, the US government in 2015 announced the Precision Medicine Initiative. Its goal is to "enable health care providers to tailor treatment and prevention strategies to people's unique characteristics"[81].

As promising as it is though, sequencing genomic data can lead to a series of privacy threats which arise from the specific properties of DNA. The most important threat to privacy is the fact that DNA is unique and it is proven very difficult to anonymize[82]. On top of that, one's DNA contains sensitive information about her, such as the disease susceptibility to various physical and mental diseases or a presumption on the racial and ethnic origin. Hence, baring specific circumstances, the patient might

[78] Chapter written by Alexandros Mittos, Section 4.5.3 by Harald Zwingelberg.
[79] Katsnelson, Alla. "Momentum grows to make 'personalized' medicine more 'precise'." (2013): 249-249.
[80] https://www.genomicsengland.co.uk/the-100000-genomes-project/
[81] https://allofus.nih.gov/
[82] S. Bradley. Realistic dna de-anonymization using phenotypic prediction. 2015.

become the victim of genetic discrimination. The problem is greatly enhanced by the fact that DNA remains mostly unchanged over the years. This means that even in the span of decades a potential breach might affect one's privacy. Last but not least, one's DNA does not reveal information only about her, but it reveals information about her relatives. This might very well influence the life for potential offspring for many decades. This fact intricates the problem since it raises the question of whether one has the right to donate or publish her genome to the public.

Indeed, recent works have proven that the patients' privacy can be compromised. In 2008, Homer et al.[83] showed that patients participating in GWAS can be identified even if their data is disseminated in an aggregated form. The above resulted in various agencies, including the National Institutes of Health (NIH), to remove the aggregated results of their research from public access.

Ultimately, we observe two distinct facts. The advances of the biomedical community in conjunction with the tendency to create and store hundreds of thousands of sequenced genomes (a) will have an immense impact on the quality of services available to patients worldwide and (b) has the potential to become a massive privacy liability to the DNA donors and their relatives. These facts give birth to the question: Can we reap the low-hanging fruits precision medicine offers without compromising the privacy of the patients? To answer this question the community of genomic privacy was born. Consisting of members from the computer science, the biomedical, and the legal community, it tries to solve this problem.

4.5.2 Protection Targets

Due to the complicated nature of genomic data, we identify a series of privacy targets. The main challenge in Genomic Privacy arises from the fact that, the goal is not to make this information unreachable, but to achieve as high utility as possible (biomedical studies, enabling physicians to use this information for the good of the patient, etc.) without breaching the privacy of the donors, and without exposing them to any potential future threat.

Table 7 Privacy protection targets for genomic privacy

	Genomic Privacy	Related GDPR articles
Confidentiality: *Data and services that process such data cannot be accessed by unauthorized entities*	Long Term Security: Most encryption methods are considered secure for the next 20-30 years. This is enough for many types of classified data (since even classified files are being opened after some decades) but this is not enough for genomic data. Genomes are immutable, and they include information not only about an individual, but about their potential offspring as well. If one's genome becomes public in the distant future, this constitutes a potential privacy breach for them and their relatives.	Art. 5 (1) (c) and (e), 17, 22, 25
Availability: *Access to (privacy-relevant) data and to services that process such data is always granted in a comprehensible, processable, timely manner*	Locale of Genomic Data: Should the user be the one who stores her genomic data (smartphone, HDD/SSD etc.) or should genomic data be held in biorepositories (cloud)? Literature has provided solutions for both options. Storing information on the cloud helps usability, as in the case of an emergency the patient's genome is easier accessible. On the other hand, storing genomic information in a personal device solves the issue of long-term security.	Art. 5 (1) (e) 13, 15, 25, 32

[83] Homer, et al., 2008..

	Medical Access: Should one's physician be able to access one's genome without her consent? The intuitive answer is no, but in real-life scenarios a physician should be able to run multiple tests based on a variety of variables. This enables a physician to conduct, for example, a personalized medicine test, to see if X drug will be efficient on the patient or not. The way a test does this is by checking specific "mutations" (also known as SNPs) in the patient's DNA. Ideally, the physician should be allowed to check only the presence of these mutations. However, in real-life scenarios, the physician might want to do further tests, as he/she thinks them necessary. Stripping him of this option would result in loss of utility, but protects the privacy of the user.	
Transparency *all privacy-relevant data processing − including the legal, technical, and organizational setting − can be understood and reconstructed at any time.*	The data subject must always know by whom and for which purposes the data is processed (collected, stored deleted, or otherwise processed). Likewise must the controller know if genomic data under its responsibility is being accessed and by whom and for what purpose and keep sufficient record of such transactions as to be able to fulfil access requests informing in detail about the recipients, Art. 15 (1) (c) GDPR. Consent must be explicit, thus clearly stating that genomic data will be processed and the purposes must be specified, see Art. 6 (2) (a) GDPR.	Art. 5 (1) (a), 6 (2) (a), 13 et seq., 25, 35
Unlinkability *privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.*	Institutes must process the contents of biorepositories, to provide aggregate information, in a privacy-preserving manner. The results must not be linkable to a specific individual (i.e. Differential Privacy) Any data shared with other institutes should be unlinkable (unless required otherwise by the research itself – cf. German cancer register)	Art. 5 (1) (c) and (e), 17, 22, 25
Integrity *data and services that process such data cannot be modified in an unauthorized or undetected manner*	Genomic data, having the potential risks and influences stated already, must in particular be correct. Measures to ensure the integrity of the data such as hash values must be in place.	
Intervenability *intervention is possible concerning all ongoing or planned privacy-relevant data processing*	Where users become empowered to store and manage their genomic data themselves e.g. on local devices, the data subjects rights do not require specific measures to be taken but the system should support users e.g. for securely storing the data or deleting it from a device before disposing it. Where genomic data is stored externally the controller must ensure effective enforcement of data subjects rights.	

4.5.3 Legal considerations on genomic privacy

Genomic data is sensitive based on a series of its attributes. It allows conclusions about e.g. heath status and risks, physiological attributes but may also allow conclusions on racial and ethnic origin. In additions the risk of abuse of these information is not limited to the person of the affected data subject but also to next in kin sharing the genetic material. Consequently Art. 9 (1) GDPR now expressly includes genetic data into the set of named special categories of personal data. A definition is provided in Art. 4 (13) GDPR.

In relation to other personal data the processing of special categories of personal data are subject is generally prohibited unless a legal ground specific to special categories of data exists. Some of these legal grounds are listed in Art. 9 (2) GDPR. This paragraph is special in relation to Art. 6 GDPR and therefore excludes as lex specialis the legal grounds provided there. In particular it is not permitted to recourse to Art. 6 (1) (f) GDPR.[84] So processing of genomic data must not be based on a balancing test between legitimate interests of the controller that are not overridden by interests of the data subject. In consequence collection of genomic data should usually be based on informed and explicit consent, stating clearly that genomic data is involved. From the specific permissions in Art. 9 para. 2 GDPR lit. (h) can be relevance for genomic data where it is processed for purposes of preventive medicine.

However, secondary use is not per se prohibited by Art. 9. In art 6 (4) GDPR the law includes a reference to special categories of data, opening secondary use clause for compatible purposes. Viewing the risks and possible consequences for the involved data subjects such secondary use will generally only be possible in a limited cases. Transfer of genetic data to third parties without previous explicit consent[85].

In the specific interest field of Privacy&Us genomic data raises some aspects in the area of transparency that require interdisciplinary attention. Besides the aspects of explicit consent, covered by legal literature already some further questions arise. One of which is the question to which extend data controllers processing genomic data must keep track of all transfers of personal data, including those to processors. Given the extreme sensitivity of genomic data a high potential interest of the data subject to contact all entities holding this data e.g. for access and rectification requests the controller should keep detailed record of recipients, including contact data. The choice between providing detailed contact data and only categories of recipients usually given to the controller[86] would provide the controller with a possibility to impede data subjects from seeking the reliefs expressly provided by Art. 16 et seq. GDPR. As these data subjects rights are a very central element and cornerstone of the GDPR and having regard to the elevated risks involved with the processing of genomic data extending to relatives of the data subject controllers handling genomic data must keep detailed record about all receivers of genomic data and also request the same from these receiving entities. In terms of usability and transparency enhancing solutions deploying ideas such as the data track presented in the PrimeLife project[87] or the specifications for handling privacy preferences together with the relevant data to be developed by the SPECIAL project[88] may provide paths for further investigation. Both responsibly acting data controllers and data subjects could benefit from tools of this type.

4.5.4 Chapter Summary

Overall, we observe two distinct facts. i) The current biomedical advances can drastically improve the treatment of patients, however, ii) this can also pose a privacy threat to the users who sequence their genome. We have identified the privacy targets and how they are being linked with the GDPR.

[84] Schluz in Gola Art. 9 DSGVO para. 1.
[85] Schluz in Gola Art. 9 DSGVO para. 6.
[86] Franck in Gola Art. 15 DSGVO para. 10; Paal, Pauly (eds.) Art. 15 para. 26.
[87] Wästlund, Fischer-Hübner (eds.) Primelife D4.2.2..
[88] See: https://www.specialprivacy.eu

5 Conclusions and Outlook

In the further course of the Marie Skłodowska-Curie innovative training network Privacy&Us this report will be the basis for a further risk assessment in the respective application areas addressed by the ESRs. Insofar this report is only an interim-step.

In respect to the GDPR this document showed that usability aspects will be more important for data protection in the future. As identified in chapter 2 the protection goal of transparency is highly related to usability aspects and as transparency requirements had been sharpened in the GDPR, usability considerations will yet become more relevant, e.g. the regulation now clearly demands that declarations must be presented in an easy language. While looking at the application domains it further showed, that not only the law became more rigid but that also the systems and processes become harder to understand by increasing complexity. It e.g. poses a challenge to understandably explain cloud computing. In the field of IoT one often faces devices missing input and output devices such as a screen forcing to recourse to external devices.

6 Literature

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information. Science, 347(6221), 509–514.

Alani, M.M. (2016). Elements of Cloud Computing Security, Available at: http://link.springer.com/10.1007/978-3-319-41411-9.

Albrecht/Jotzo: Jan Philipp Albrecht, Florian Jotzo; Das neue Datenschutzrecht der EU; Nomos, Baden-Baden, 2017

Antignac, T., & Le Metayer, D. (2014). Privacy by Design: from technologies to architectures. Privacy Technologies and Policy, 8450, 1–17. http://doi.org/10.1126/science.1143464

Art. 29 WP 100: Article 29 Data Protection Working Party(2004). Working Paper 100, "Opinion 10/2004 on More Harmonised Information Provisions", Adopted on 25th November 2004, online: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf

Art. 29 WP 196: Article 29 Data Protection Working Party (2012), "Opinion 05/2012 on Cloud Computing", Working Paper 196, Adopted July 1st 2012, online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Art. 29 WP 196: Article 29 Data Protection Working Party (2912). "Opinion 05/2012 on Cloud Computing", Working Paper 196, Adopted July 1st 2012, online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Art. 29 WP 248: Article 20 Data Protection Working Party (2016). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, Adopted on 4 April 2017, online: file:///C:/Users/hzwingelberg/Downloads/wp248_enpdf%20(4).pdf

B Paal, B. P., Pauly, D. A. (2017). Datenschutz-Grundverorndung – DS-GVO, Munich 2017.

Barkhuus, L. (2012). The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. ACM SIGCHI Conference on Human Factors in Computing Systems, 367–376. http://doi.org/10.1145/2207676.2207727

Bettini, C. & Riboni, D. (2015). Privacy protection in pervasive systems: State of the art and technical challenges. Pervasive and Mobile Computing, 17(PB), pp.159–174.

Brown, B. Studying the Internet experience. . s.l. : HP Laboratories Technical Report HPL, 2001.

Bruening, P. J., & Culnan, M. J. (2015). Through a Glass Darkly : From Privacy Notices to Effective Transparency. Nroth Carolina Journal of Law & Technology, (June), 1–46.

Chang, V., Kuo, Y.-H. & Ramachandran, M. (2015). Cloud Computing Adoption Framework: a security framework for business clouds. Future Generation Computer Systems, 57, pp.24–41.

Choi, B., & Tam, J. (2015). Privacy by design: examining two key aspects of social applications. HCI in Business, 9191, 437–445. http://doi.org/10.1007/978-3-319-20895-4

Commission, European. Special Eurobarometer 431 “Data Protection.” . s.l. : European Commission, 2015.

Cook, 2014: D. and Das, S.K. (2004). Smart Environments: Technology, Protocols and Applications., John Wiley & Sons.

DSK, SDM: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK, engl: °Conference of the Independent Data Protection Authorities of the Bund and the Länder) (2016). The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals, online: https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html

European Data Protection Supervisor (2017). 'EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)' (Opinion 6/2017) 24 April 2017, online: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf.

Fazio, M. et al. (2015). Big Data Storage in the Cloud for Smart Environment Monitoring. In The 6th International Conference on Ambient Systems, Networks and Technologies (ANT2015). Elsevier Masson SAS, pp. 500–506.

Fischer-Hübner, S., Petterson, J. S., Angulo, A. (2015). HCI Requirements for Transparency and Accountability Tools for Cloud Services, in: Accountability and Security in the Cloud, First Summer School, Cloud Accountability Project, A4Cloud, revised selected papers, Cham, 2015.

GDPR. (2016). Retrieved 02 02, 2017, from EU general data protection regulation: http://eur-lex.europa.eu/legal- content/EN/TXT/HTML/?uri= CELEX:32016R0679&from=EN

Homer, et al. (2008). Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays. PLoS Genet, 4(8), p.e1000167

ITU-T, R: ITU-T, R., 2014. ISO/IEC 17788 - Information technology - Cloud computing - Overview and vocabulary. , (Y.3500), pp.1–16.

Jacobsson, A., Boldt, M. & Carlsson, B., (2014). On the Risk Exposure of Smart Home Automation Systems. International Conference on Future Internet of Things and Cloud (FiCloud), pp.183–190.

Kelley, P., Cesca, L., Bresee, J., & Cranor, L. (2010). Standardizing privacy notices : an online study of the nutrition label approach. Human Factors in Computing Systems, 1573 – 1582. http://doi.org/10.1145/1753326.1753561

Kühling, J, Buchner, B (eds.) (2017). Datenschutzgrundverordnung - Kommentar, Munich, 2017.

Langheinrich, M. et al. (2004). Living in a Smart Environment: Implications for the Coming Ubiquitous Information Society. In 2004 IEEE International Conference on Systems, Man and Cybernetics. IEEE.

Lauristin, M. (2017) Draft report on the 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), online: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

Madden M., Rainie L. Americans' attitudes about privacy, security and surveillance. s.l. : Pew Research Center, 2015.

Monteleone, S., Bavel, R. Van, Rodríguez-Priego, N., & Esposito, G. (2015). Nudges to Privacy Behaviour: Exploring an Alternative Approach to Privacy Notices. http://doi.org/10.2791/142795

Nauman, M., Khan, S., and Zhang, X. (2014). Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help?. in Proceedings of the 23th International Conference on World Wide Web, China, pp. 201–212.Norberg, P. A., Horne, D. R., The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors, The Journal of Consumer Affairs, 2007, Vol. 41.

NIST 2011: Mell, P. & Grance, T., 2011. NIST definition of cloud computing, Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Reidenberg, J. R., Breaux, T. D., Cranor, L. F., French, B., Grannis, A., Graves, J. T., … Schaub, F. (2015). Disagreeable privacy policies: mismatches between meaning and users' understanding. Berkley Technology Law Journal, 30(1), 39–68.

Rost, M., Pfitzmann, A. (2009) Datenschutz-Schutzziele Reconsidered, in DuD 2009, p. 353 – 358.

Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A Design Space for Effective Privacy Notices. In Symposium on Usable Privacy and Security (SOUPS) 2015 (pp. 1–17). Ottawa, Canada.

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. Computers in Human Behavior, 55, 992–1000. http://doi.org/10.1016/j.chb.2015.09.038

Wästlund, E., Fischer-Hübner, S. (2010). End User Transparency Tools: UI Prototypes, PrimeLife

project deliverable D4.2.2, online: http://primelife.ercim.eu/images/stories/deliverables/d4.2.2-transparency_tools_ui_prototypes-public.pdf

Wei, X. (2013). Understanding and improving the smartphone ecosystem: measurements, security and tools. Doctoral Dissertation. University of California.

Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), pp.583–592.

Zuiderveen Borgesius, F. (ed.), van Hoboken, J., Fahy, R., Irion, K., Rozendaal, M. (2017). An Assessment of the Commission's Proposal on Privacy and Electronic Communications, - Study for the LIBE Committee, European Parliament, 2017, online: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN^.