POST PRINT VERSION
Saltarella, M., Desolda, G., Lanzilotti, R., & Barletta, V. S. (2023). Translating Privacy Design Principles Into Human-Centered Software Lifecycle: A Literature Review. International Journal of Human–Computer Interaction, 40(17), 4465–4483. https://doi.org/10.1080/10447318.2023.2219964

Translating Privacy Design Principles into Human-Centered software lifecycle:

A Literature Review

Marco Saltarella[a,b], Giuseppe Desolda[a], Rosa Lanzilotti[a], Vita Santa Barletta[a]

[a] Dipartimento di Informatica, Università degli Studi di Bari Aldo Moro, Bari, Italy

[b] FINCONS SpA, Bari, Italy

Abstract

Companies and organizations involved in software development are stimulated and often obliged to consider procedures and technical solutions to guarantee data privacy and protection from the early phases of the software lifecycle. In addition, by default, personal data might be processed with the highest privacy protection level. These two requirements are Privacy by Design and Privacy by Default principles. Their importance has grown quickly in the last few years, as demonstrated by data protection regulations, like GDPR and PIPEDA, which include them as an important part of some of their articles. However, such regulations do not provide any practical or concrete indications of software requirements, and developers often lack adequate knowledge to understand the privacy prescriptions expressed in legal language. This study addresses these limitations by presenting a systematic and rigorous literature review that aims to answer the following research questions: RQ1) How do Privacy-By-Design and Privacy-By-Default principles translate into software requirements? and RQ2) How Privacy-By-Design and Privacy-By-Default principles integrate into a Human-Centred Design process? For RQ1, the analysis of the resulting publications led to identifying several software requirements and business processes organized along 8 data-oriented and process-oriented privacy design strategies. For RQ2, the analysis of the retrieved publications provided a comprehensive view of the HCI methodologies adopted to comply with privacy requirements identified current shortcomings, and proposed future research directions. The results have been distilled into an initial framework that may aid the development of software that must comply with such principles and aims to integrate them into an HCD process.

Keywords: privacy by design; privacy by default; privacy design strategies; human-centered design approach

Translating Privacy Design Strategies into Human-Centered software lifecycle: A Literature Review

Introduction

Privacy by Design and Privacy by Default are conceptual principles for software development that require initiating a project by providing, from the outset, the right tools and settings to protect personal data. The concept of Privacy by Design dates back to the ’90s and was coined by Ann Cavoukian, then Privacy Commissioner of Ontario, Canada (Cavoukian, 2009). This principle puts the final user at the center of the development process from a privacy perspective, obligating the data controller to effective protection from a substantive, not just a formal, point of view. The principle of Privacy by Default states that the software, by default, uses only personal data to the extent necessary and sufficient for the intended purposes and the period strictly necessary for those purposes. This imposes to design data processing systems ensuring reasonable data collection so that the users receive a high level of protection even if they do not take action to limit data sharing.

These principles are strongly influencing the data protection regulations released in several countries. For example, the GDPR (General Data Protection Regulation) is the European Union’s data privacy regulation that mandates strict personal data life-cycle governance requirements. In Article 25, the GDPR demands that clear organizational and technical measures must be implemented to guarantee specific principles and rights to data subjects. Such measures must also be implemented following the “by design” (security and privacy should be considered from the earliest design phase of a system) and “by default” (the system should be configured as secure and privacy-preserving as possible) principles. In the USA, there is no analogous to GPDR, but there are sector-specific data protection laws and regulations (e.g., Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, Federal Information Security Management Act) that include similar principles. Also in Canada, the protection of personal data is regulated by two federal laws: Personal Information Protection and Electronic Documents Act (PIPEDA), respectively, for the private and public sectors. Although the current release of these regulations does not explicitly mention these principles, their commissions recently started discussing their introduction in the following versions (Canadian Standing Committee on Access to Information, Privacy and Ethics, 2018).

Despite the proliferation of data regulations that include Privacy by Design and Privacy by Default principles as an essential part of their articles, there are still important open issues and challenges that limit the wide and proper adoption of such regulations. First, there is still a lack of knowledge on how to translate such principles into concrete requirements for software development, e.g., how to layer the application, how to design the database, how to create classes and packages, and how to design the user interface and user interaction. Second, data privacy is perceived as can be a daunting task (O’Connor et al., 2017), especially by developers who lack a basic understanding of both the legal and security concepts expressed in the regulation (Martin & Kung, 2018). While some attempts have been made to partially address this issue (for example, (Hadar et al., 2018; Lodge & Crabtree, 2019; Martin & Kung, 2018)), there is no clear and complete view of this challenge. Third, it is crucial to understand how the implementation of security mechanisms required by regulations affects the system usability to avoid overburdening the user and ensure proper interaction (Pattakou et al., 2018), which is an aspect scarcely investigated before. In this regard, Human-Computer Interaction (HCI) methodologies can help shed light on the user-effective and compliant implementation of privacy and security technologies (Iachello & Hong, 2007).

To overcome these limitations identified in the literature, this study aims to contribute to the state-of-the-art by investigating i) how Privacy-By-Design and Privacy-By-Default principles translate into software requirements and ii) how Privacy-By-Design and Privacy-By-Default principles integrate into a Human-Centred Design (HCD) process. This is achieved by performing a systematic literature review (SLR) on the state-of-the-art solutions that address these principles. After defining a rigorous research protocol in line with the guidelines proposed by Kitchenham (Kitchenham, 2004), more than 1900 publications were collected from the major digital libraries. Each publication was analyzed and assessed through specific inclusion criteria in an iterative process to identify relevant publications that answer the defined research questions.

The analysis of the SLR has been distilled into a framework that supports the design and development of software that must adhere to Privacy-By-Design and Privacy-By-Default principles and aims to incorporate them into an HCD methodology. Specifically, it proposes two main contributions. First, it identifies a set of software requirements and business processes for Privacy-By-Design and Privacy-By-Default by mapping state-of-the-art solutions to eight data-oriented and process-oriented privacy design strategies (Hoepman, 2014). This will help stakeholders to speed up, improve the quality and concretise the translation of such principles into software requirements, avoiding misinterpretations, standardising modus operandi and ensuring high quality of implemented solutions. Second, it provides a clear and comprehensive view of the HCI methodologies used to meet privacy requirements and the challenges in their implementation. This will contribute to a more user-centric implementation of software requirements, even for those who are not necessarily HCI experts, as the proposed mapping suggests what the best HCI solutions at different stages of software development are.

Paper outline

To present the results of this work, the remainder of this paper is organized as follows.

The following section presents the related works and the background in order to frame this research and briefly highlight current shortcomings in the literature.

Afterwards, the methodology followed for this systematic literature review is reported, including the formulation of the research questions, the definition of the search strings and the inclusion criteria.

Then, the results of the review are presented and analysed under different dimensions trying to answer the identified research questions.

Finally, four different inputs for further research activities are illustrated together with the conclusions and future work to be undertaken conclude the article.

Background and Related Work

Privacy in IT organizations

Data privacy is a broad concept that concerns the ability of individuals or organisations to control and protect their personal or confidential information from unauthorised access, use or disclosure. It also refers to ensuring that data is collected, processed, stored and shared securely and transparently, with explicit consent and in an appropriate legal and ethical manner. Data protection is one of the most critical aspects of cybersecurity because it helps prevent identity theft, fraud and other malicious activities that can harm individuals, businesses and society as a whole (European Network and Information Security Agency, 2014). They require specific methodologies, tools, and techniques for data processing to reduce security incidents that can seriously threaten information privacy.

Privacy Enhancing Technologies (PETs) are emerging solutions to improve privacy protection in IT organizations. PETs can be used to solve some of the key challenges in privacy risk mitigation and system design (European Network and Information Security Agency, 2014). However, PETs need to be rooted in a data governance strategy to be applied in practice and, in addition, this represents only one element to be considered within the system life cycle: it is necessary to understand at each phase of development or reengineering how to operationally translate Privacy by Design principles and guidelines (Baldassarre et al., 2020).

Different contributions have been made to outline universal standards and principles that support IT organizations. In 2009, the International Data Protection and Privacy Commissioners Conference defined a set of principles and rights for the effective and international uniform protection of privacy in the processing of personal data and the facilitation of the international flows of personal data needed in a globalized world (Rallo Lombarte, 2009). These represent core principles for privacy by design, which emerges as a proactive and integrative approach to strengthening privacy requirements early in application design (Regulation (EU) 2016/679, 2016). During that conference also, the following properties emerged: *Unlikability*, i.e., privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context; *Transparency*, i.e., all privacy-relevant data processing can be understood and reconstructed at any time, including legal, technical and organizational setting; *Intervenability*, i.e., intervention is possible concerning all ongoing or planned privacy-relevant data processing (Hansen et al., 2015).

As a further contribution, in 2011 the ISO/IEC 29100 was published by International Organization for Standardization and International Electrotechnical as an international standard (International Organization for Standardization, 2011). It proposes a privacy framework targeted to organizations and intended to support them in defining their privacy-safeguarding requirements related to personally identifiable information (PII), specifying a common privacy terminology, defining the actors and their roles in processing PII, describing privacy requirements and referring know privacy principles.

Privacy by design and privacy by default

The GDPR is one of the regulations providing the most comprehensive rights for citizens. However, privacy was well-discussed before the GDPR was enacted in May 2018. Indeed, one of the most influential studies in the matter of privacy is proposed by Cavoukian (Cavoukian, 2009), where the following 7 foundational privacy by design principles were defined:

1) *Proactive not Reactive*: it asks for trying to prevent and be proactive concerning a privacy issue that may arise instead of mindlessly waiting for the risk to materialize;

2) *Privacy as the Default Setting*: it means that, by default, the system should be configured with the most privacy-preserving setting by default;

3) *Privacy Embedded into Design*: it implies that privacy should be seen as a process throughout the whole design process of the system and not just in some random timeframe;

4) *Fully Functionality – Positive-Sum, not Zero-Sum*: it means that developers should try to accommodate all the interests of the involved stakeholders of the system and try to maximize both functionality and privacy;

5) *End-to-End Security – Full Lifecycle Protection*: it means that data should be protected throughout their whole lifecycle, from when data are created until they are destroyed;

6) *Visibility and Transparency – Keep it Open*: it asks for being transparent about the personal data processing to promote the system's trustworthiness;

7) *Respect for User Privacy – Keep it User-Centric*: the ultimate goal should be to protect the privacy of the involved users. It should be done by adopting a user-centred approach to help users make an informed decision about their privacy.

A careful reader may realize that these principles can be found, in one way or another, in the GDPR. For example, article 5 asks for lawfulness, fairness and transparency as well as integrity and confidentiality of data; likewise, article 25 itself asks for adopting the by-design and by-default approaches.

These principles represent the foundation of the Privacy by Design approach aiming at embedding privacy and security into Information and Communications Technology (ICT) processes and architectures. Under this paradigm, privacy should be conceived as an integral part of the information systems meaning that systems architecture must be designed to consider not only technical but also security and privacy requirements. The concept of Privacy by Design is strictly related to the one of Security by Design, which is an older paradigm mostly based on purely technical principles: Confidentiality, Integrity and Availability (CIA), which means that only authorized entities should be able to access information (confidentiality), information should be protected against unauthorized modification or erasure (integrity), and information should always be available when requested by an authorized entity (availability). According to Cavoukian and Chanliau, privacy and security by default paradigms should converge into a single concept given that these paradigms complement and mutually reinforce each other (Cavoukian & Chanliau, 2013).

As technology but also users' privacy expectations and related regulations evolve, it is necessary to reconsider how systems are designed and start to proactively integrate privacy by default (Cavoukian & Dixon, 2013). Indeed the "by-default" approach is also strictly intertwined with the "by-design" paradigm. This paradigm asks for implementing different security policies to ensure the system is configured in the most secure setting possible. These policies include the principles according to which the authorization privileges, the trust, and the information accessed should be reduced to the minimum possible to minimise the risk associated with security attacks. Indeed, it is clear how Cavoukian's work represented a milestone in the literature serving as inspiration and a solid foundation on which our current regulation is based.

However, while these by-design and by-default paradigms propose high-level principles to reconsider the system design process, it is also important to understand how these paradigms can be practically implemented in everyday practices, which could be not that straightforward. One way discussed in research to implement privacy measures are reusable components, including techniques, tools, and methodologies. For example, in (Caiza et al., 2019), the authors provide a mapping study to provide reusable components for designing privacy-aware systems. However, the authors highlight that despite this research field getting more and more interest over time, most of the contributions analyzed still lack empirical evidence and remain just solution proposals and, thus, are not mature enough to be adopted in practical scenarios. This view is further corroborated in (Lenhard et al., 2017) in which the authors, after analysing literature contributions in privacy engineering, state that although patterns could help support GDPR compliance, research still provides few practical guidelines for practitioners. Thus, there is still work to be done to strengthen the available privacy patterns by empirical evaluation.

In (Colesky & Caiza, 2018), the authors provide a set of patterns focused mainly on informing users about data processing contributing to an already promising catalogue of privacy patterns[1]. The patterns proposed in the article help users make informed decisions and understand the risks in consenting to data processing, supporting the transparency principle according to the informed privacy design strategy. However, as already reported by one of the authors of the paper, there is a need to enhance the application of privacy design strategies in processes, guidelines and methodologies (Caiza et al., 2019). On the other hand, there are also the so-called dark patterns (Fritsch, 2017), the antithesis of privacy design patterns and Hoepman's privacy design strategies, which purposely violate privacy requirements. Although their usefulness might be controversial, the dark patterns help raise awareness, as they each propose effective countermeasures that users can adopt in the described situations.

In (Kurtz & Semmann, 2018), after having reviewed the literature on Privacy by Design approaches, the authors suggest an agenda to foster the research on GDPR requirements implementation. Specifically, they propose to identify and validate the privacy by design

[1] http://privacypatterns.org

requirements to comply with the regulation, develop benchmarks for evaluating the data processing lifecycle, and develop supporting tools to help engineers integrate GDPR compliance to foster transparency ultimately. However, this work only focuses on Cavoukian's Privacy by design principle of visibility and transparency, leaving out other concerns regarding the remaining principles.

Starting from these considerations found in the literature, this work aims to identify more technical approaches, which are less abstract and more practical, on how to design and develop GDPR-compliant software, following the privacy by design and default paradigms considered effective ways to implement more user-centric privacy-aware solutions.

Methodology

The research protocol used for conducting the SLR was defined following the guidelines proposed by Kitchenham et al. (Kitchenham, 2004). The following phases were carried out:

- **Planning**: definition of the research questions, identification of relevant keywords, and definition of the inclusion and exclusion criteria;
- **Conducting**: retrieval of publications from the main research engines and iterative selection of the studies according to the defined inclusion and exclusion criteria;
- **Reporting**: extraction and discussion of relevant results to address the research questions.

The planning and conducting phases are described in the following subsections, while the reporting phase is described in the next section.

Planning phase

Formulation of the research questions.

The first activity was defining the research questions, which aimed to address the goal of this SLR, i.e., to systematize the current best practices of privacy-compliant software design and development implementing privacy-by-design and privacy-by-default paradigms. We formally expressed and detailed the overall goal of this study in the following research questions:

RQ1) How Privacy-By-Design and Privacy-By-Default principles translate into software requirements?
RQ2) How Privacy-By-Design and Privacy-By-Default principles integrate into an HCD process?

RQ1 focuses on identifying technical and practical solutions at the state-of-the-art that can translate the Privacy-By-Design and Privacy-By-Default principles into requirements to ease software development. RQ2 aims to determine how these principles can be included in an HCD process, which is essential to involve users along the software life cycle.

Definition of the search strings.

The search strings are the backbone of the SLR. It is a comprehensive list of keywords and phrases used to identify studies relevant to the research questions. To identify the most relevant studies to answer our RQs, a combination of key terms was set up. First, we identified general-purpose terms that fit both the RQs, i.e., *Data Protection Regulation*, *privacy*, *privacy by design,* and *privacy by default*. Then, for each RQ further terms, more specific for each RQ, have been identified. Specifically, for RQ1 the selected terms were engineering, guidelines and patterns, and informed consent. The resulting search string for RQ1 was:

“Data Protection Regulation” AND (privacy OR “privacy by design” OR “privacy by default” OR security OR software) AND (engineering OR guidelines OR “informed consent” OR patterns)

Similarly, since RQ2 wanted to highlight the relationship between privacy by design and default approaches under the different privacy regulations and the Human-Computer Interaction field, the following terms were also selected: *usability*, *usable privacy*, *Human Factors* and *user-centric*. Thus, the resulting search string was:

“Data Protection Regulation” AND ("privacy by design" OR "privacy by default") AND ("usability" OR "usable privacy" OR "usable security" OR HCI OR CHI OR "Human Factors" OR "Human Interaction" OR "user-centric").

It should be noted that the terms chosen are deliberately quite generic, so that when querying the data sources there is a greater chance of retrieving a wide range of publications, which can then be manually filtered according to the inclusion criteria. Conversely, forcing the presence of more specific terms (e.g. GDPR, PIPEDA, policies, frameworks) could result in interesting papers not being retrieved.

Selection of data sources.

The search strings were used to query 4 major digital libraries: ACM DL, IEEE Xplore, Scopus, and Google Scholar. The research strings were provided as input to these digital libraries following the specific syntax required by each research engine: this meant using the double quotes to link together words like human factors or privacy by design, which had to appear in the text one after the other in the same order, and proper use of Boolean operator and parenthesis, except the ACM Digital library that required the “+” symbol instead of AND.

Definition of Inclusion criteria.

To select publications that fit the research questions, inclusion criteria were defined to ensure an unbiased selection of relevant publications. Therefore, a publication was retained if it satisfied all the following criteria:

- IN1: the publication focuses on the implementation of privacy-by-design and/or privacy-by-default principles;
- IN2: the publication is related to ICT or HCI topics;
- IN3: the publication is published in a relevant journal or conference;
- IN4: the publication has been peer-reviewed;

Conducting phase

The search strings used on the 4 digital libraries allowed us to retrieve more than 1900 publications. In particular, the execution of the RQ1 search string retrieved 1440 publications (ACM DL = 60, IEEE Xplore = 369, Scopus = 673, Google Scholar = 338). From these publications, 417 resulted duplicated and thus removed, obtaining a total of 1023 publications to be considered for review.

The execution of the RQ2 search string retrieved 508 publications (ACM DL = 202, IEEE Xplore = 140, Scopus = 17, Google Scholar = 149). From this set of publications, 43 were removed because duplicated, thus resulting in a total of 465 publications. A total of 1948 publications were retrieved, and this phase finished in March 2023.

From this point on, an iterative selection process was conducted by applying inclusion criteria. First, publications were analyzed based on their title and abstract only. The application of the criteria to the RQ1 publications allowed us to exclude 912 publications. After that, a more detailed analysis was conducted by reading the whole manuscript, leading to the selection of 111 publications. The application of the criteria to the RQ2 publications allowed us to exclude 436 publications. After that, reading the full texts, 29 publications were selected. Figure 1 summarizes the search phases while all the details of these phases, and all the results, can be found at https://bit.ly/3WzHOOv.

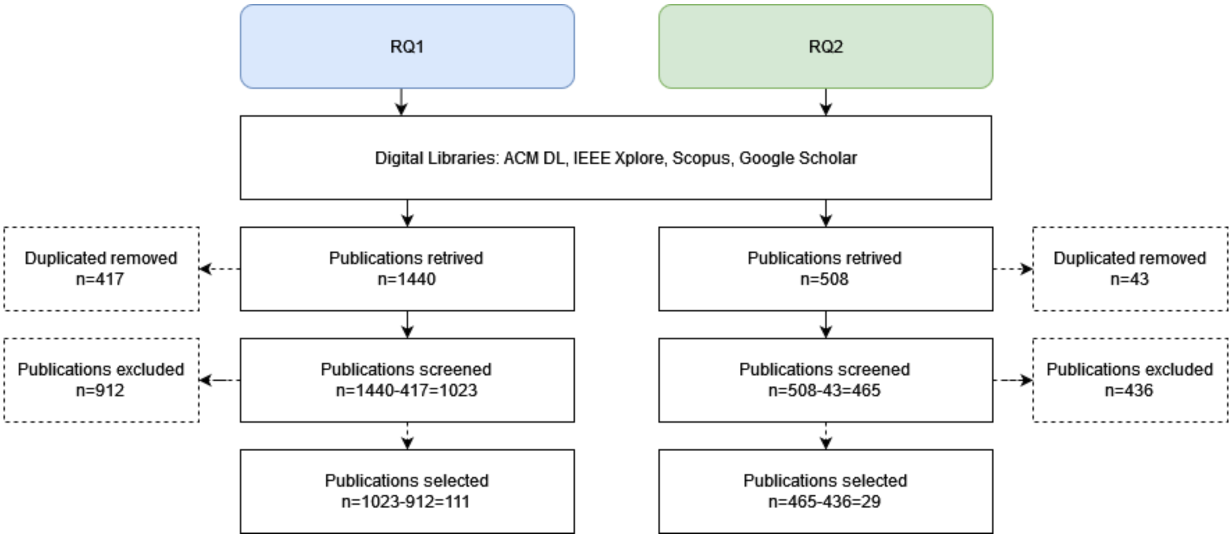
RQ1
RQ2
Digital Libraries: ACM DL, IEEE Xplore, Scopus, Google Scholar
Duplicated removed n=417
Publications retrived n=1440
Publications retrived n=508
Duplicated removed n=43
Publications excluded n=912
Publications screened n=1440-417=1023
Publications screened n=508-43=465
Publications excluded n=436
Publications selected n=1023-912=111
Publications selected n=465-436=29

Figure 1 Flow diagram summarizing the selection of the publications along the search phases.

Reporting and Analyzing the SLR Results

This section reports the analysis of the SLR results framed along the two research questions presented in the previous section. The answers to these research questions, which are distilled in Table I and Table II, offer an initial framework to facilitate the development of software that needs to comply with Privacy by Design and Privacy by Default principles and aims to integrate them into an HCD process. In the following, we report on the results and analysis of the two

RQs.

How Privacy-By-Design and Privacy-By-Default principles translate into software requirements? (RQ1)

To frame the analysis of the 111 publications selected for RQ1, we adopted the “Privacy Design Strategies” (Hoepman, 2014), where 8 different strategies are defined. These 8 strategies are divided into two sub-categories:

1. Data-oriented strategies focused on the data processing itself:
    - *Minimize*: reduce the amount of data collected and processed to the minimum;
    - *Separate*: distribute data processing and storage;
    - *Abstract*: limit the detail level of data processing as much as possible;
    - *Hide*: personal data should be hidden from unauthorized third parties;
2. Process-oriented strategies focused on the process handling the personal data lifecycle:
    - *Inform*: duly inform the users about the whole data processing lifecycle;
    - *Control*: empower the users with complete control over their personal data;
    - *Enforce*: enforce privacy-friendly data processing;
    - *Demonstrate*: demonstrate the enforcement of privacy-friendly data processing;

These privacy design strategies provide a high-level approach to improving the privacy of a system. Indeed, privacy design strategies suggest decisions from a strategic point of view, providing input on what should be achieved at a data and process level to ensure the design of a privacy-preserving system. However, implementing these strategies should be done methodically and pragmatically, involving all interested stakeholders, from engineers to end users (Hoepman, 2014).

To solve these issues, we mapped the 111 publications inside the 8 strategies and, in each strategy, one or more publications were translated into requirements. For example, for the strategy “Minimize”, we identified the requirement “Display to the users only the data strictly needed to avoid unnecessary disclosure” related to the studies reported in (Colesky & Ghanavati, 2016; Morales-Trujillo & Garcia-Mireles, 2018). The complete list of strategies and requirements is discussed in the following and reported in Table I.

Table 1. Mapping of the RQ1 publications inside the 8 strategies, with a brief explanation of their contribution.

1. Minimize	
Display to the users only the data strictly needed to avoid unnecessary disclosure	(Colesky & Ghanavati, 2016; Morales-Trujillo & Garcia-Mireles, 2018)
Select carefully the data to be processed	(Colesky & Ghanavati, 2016; Kneuper, 2020; Kung et al., 2017)
Limit the collection of data to the one required for the proper functionality of the application	(Abdulghani et al., 2019; Hatamian, 2020; Kneuper, 2020)
Minimize data storage retention to reduce the risks associated with data breaches	(Abdulghani et al., 2019; Diamantopoulou et al., 2020)
2. Separate	
Adopt an MVC architecture	(Morales-Trujillo & Garcia-Mireles, 2018)
Process data in a distributed fashion through isolation and virtualization	(Colesky & Ghanavati, 2016; Kung et al., 2017; Ladjel et al., 2019)
Interconnect systems via overlay networks or message brokers	(Coroller et al., 2018; Kretschmer et al., 2021; Pedrosa et al., 2019; Rhahla et al., 2021)
Separate users’ data into sub-profile, to avoid account-wide data breaches.	(Gabel & Schiering, 2019; Pedrosa et al., 2019)
Ensure cross-domain unlikability through context separation (physical and digital)	(Gabel & Schiering, 2019; Mougiakou & Virvou, 2017)
Opt for a decentralized storage	(Abdulghani et al., 2019; Custers et al., 2018)
3. Abstract	
Employ homomorphic encryption to perform computation over encrypted data	(Abdulghani et al., 2019; Kretschmer et al., 2021; Kühtreiber et al., 2022; C. Li & Palanisamy, 2019; Notario et al., 2017)
Use Differential Privacy to query a dataset in a privacy-preserving way	(Gruschka et al., 2018; Kretschmer et al., 2021, 2021; Kühtreiber et al., 2022; Kung et al., 2017; C. Li & Palanisamy, 2019; Roig, 2018; Sokolovska & Kocarev, 2018)

Use anonymization techniques like k-anonymity, l-diversity, and t-closeness	(Abdulghani et al., 2019; Damjanovic-Behrendt, 2018; Gruschka et al., 2018; Kounoudes & Kapitsaki, 2020; Kühtreiber et al., 2022; Kung et al., 2017; C. Li & Palanisamy, 2019; Roig, 2018; Roubtsova et al., 2018; Saatci & Gunal, 2019; Sokolovska & Kocarev, 2018)
Abstract data through derivation and approximation	(Saatci & Gunal, 2019)
Aggregate data over time	(Abdulghani et al., 2019; Diamantopoulou et al., 2020; Kung et al., 2017; Mannhardt et al., 2018)
4. Hide	
Use Encryption both for storage and transfer	(Abdulghani et al., 2019; Diamantopoulou, Argyropoulos, et al., 2017; Diamantopoulou et al., 2020; Fernandes et al., 2018; Gruschka et al., 2018; Hatamian, 2020; Kung et al., 2017; Mannhardt et al., 2018; Mougiakou & Virvou, 2017; Notario et al., 2017; O'Connor et al., 2017; Papageorgiou et al., 2018; Saatci & Gunal, 2019)
Use attribute based Encryption and/or Attribute-Based Access Control	(Abdulghani et al., 2019; Coroller et al., 2018; Gabel & Schiering, 2019; C. Li & Palanisamy, 2019; Michael et al., 2019; Rhahla et al., 2021)
Use application layer protocols over TLS	(Badii et al., 2020; Hatamian, 2020; C. Li & Palanisamy, 2019)
Hide sensitive data through masking, mixing and tokenization	(Gonçalves et al., 2020; Groen & Ochs, 2019; Saatci & Gunal, 2019)
Do not log sensitive information (e.g., personal data, password etc.)	(Papageorgiou et al., 2018)
5. Inform	
Explain the process of personal data processing in a detailed, concise and understandable way.	(Ataei et al., 2018; Betzing et al., 2019; Colesky & Ghanavati, 2016; Custers et al., 2018; G Karácsony, 2019; Mohan et al., 2019; Morales-Trujillo & Garcia-Mireles, 2018; O'Connor et al., 2017; Wachter, 2018a, 2018b)
Inform users explicitly about any data collection, sharing and processing taking place.	(Ataei et al., 2018; Butin & Le Métayer, 2015; Hatamian, 2020; Mannhardt et al., 2018; Morel et al., 2019)
Inform users about which data is collected and for which duration, how to request data removal and how to withdraw consent	(Ataei et al., 2018; Butin & Le Métayer, 2015; Mannhardt et al., 2018; Mohan et al., 2019)
Asking for a user's consent for processing his/her personal data must be separated from asking consent for services offered	(Colesky & Ghanavati, 2016; Hatamian, 2020; Kneuper, 2020; Wachter, 2018b)
Employ Transparency Enhancing Tools	(Spagnuelo et al., 2017, 2019; Tapsell et al., 2018)
Use visual reminders	(Ataei et al., 2018; Custers et al., 2018; G Karácsony, 2019; O'Connor et al., 2017; Palmirani et al., 2018)
6. Control	
Specify policies in a machine-readable format and automate the informed-consent process (e.g., by using P3P, PPL or LPL)	(Gerl & Meier, 2019; Kounoudes & Kapitsaki, 2020; Kretschmer et al., 2021;

	C. Li & Palanisamy, 2019; Martucci et al., 2017; Neisse et al., 2016; Pardo & Le Métayer, 2019; Su et al., 2016)
Give users the chance to learn and practice their rights (access, rectification, erasure, giving and withdrawing consent, and portability) through system UI/dashboard	(Ataei et al., 2018; Betzing et al., 2019; Fernandes et al., 2018, 2018; Hatamian, 2020; Hyysalo et al., 2016; Kneuper, 2020; Kung et al., 2017; Mannhardt et al., 2018; Piras et al., 2019; Wachter, 2018a)
Provide consent in forms and at times that minimize users' fatigue and maximize the likelihood that they make appropriate decisions	(Ataei et al., 2018; Hyysalo et al., 2016; Morel et al., 2019; Nouwens et al., 2020; Soe et al., 2020; Utz et al., 2019)
Move away from a take it or leave it and empower the user in choosing a balance between functionality and privacy	(Custers et al., 2018; Gol Mohammadi et al., 2019; Kneuper, 2020)
Use Sticky policies	(Custers et al., 2018; Gol Mohammadi et al., 2019; Kung et al., 2017; Martucci et al., 2017)
7. Enforce	
Collect and process personal data only if the current consent given by the user covers the purpose of the collection.	(Antignac et al., 2018; Fernandes et al., 2018; Hatamian, 2020; Mustafa et al., 2019)
Use models to support GDPR compliance and verification	(Agostinelli et al., 2019; Ahmadian, Jürjens, et al., 2018; Ahmadian et al., 2019; Diamantopoulou, Angelopoulos, et al., 2017; Kupfersberger et al., 2018; Loruenser et al., 2018; Martin & Kung, 2018; Pedroza et al., 2021; Stach & Steimle, 2019; Torre et al., 2019)
Foster awareness and education for the development team but also for users	(Alhazmi & Arachchilage, 2021; Ataei et al., 2018; Campanile et al., 2022; Custers et al., 2018; G Karácsony, 2019; Hadar et al., 2018; Leite et al., 2022; Z. S. Li et al., 2020; Lodge & Crabtree, 2019; Martino et al., 2019; O'Connor et al., 2017; Singh & Cobbe, 2019)
Adopt ontologies to model information related to personal data to improve interpretation, visualization and compliance checking against privacy policies	(Bartolini et al., 2015; Besik & Freytag, 2019; Fatema et al., 2017; Olca & Can, 2022; Pandit et al., 2018)
Execute a process to regularly assess, test and evaluate the effectiveness of the technical and organizational measures concerned with the data processing	(Agarwal et al., 2018; Ayala-Rivera & Pasquale, 2018; Diamantopoulou & Mouratidis, 2019; Fernandes et al., 2018; Ferrara & Spoto, 2018; Leite et al., 2022; Z. S. Li et al., 2022; Morales-Trujillo & Garcia-Mireles, 2018; Torre et al., 2019)
Follow the Global Privacy Standard principles	(Alshammari & Simpson, 2017c)
8. Demonstrate	
Performa a Data Protection Impact Assessment	(Ahmadian, Strüber, et al., 2018; Butin & Le Métayer, 2015; Coles et al., 2018; Diamantopoulou & Karyda, 2022; Martucci et al., 2017; Mougiakou & Virvou, 2017; Mustafa et al., 2019; Sion, Dewitte, et al., 2019; Wachter, 2018a, 2018b)
Adopt a privacy threat modeling and management strategy (e.g., LINDDUN)	(Al-Momani et al., 2019; Martin & Kung, 2018; Martín & Del Álamo, 2017; Meis & Heisel, 2017; Muntes-Mulero et al., 2019;

	Sion, Dewitte, et al., 2019; Sion et al., 2018; Sion, Landuyt, et al., 2019)
Adopt a personal data-centric lifecycle model also to support the identification of critical activities and associated privacy risks	(Alshammari & Simpson, 2017c, 2017a, 2017b; Diamantopoulou & Karyda, 2022; Morales-Trujillo & Garcia-Mireles, 2018; Ujcich et al., 2018)
Keep a record of users' consent decisions and make it available on request also to ensure accountability	(Butin & Le Métayer, 2015; Diamantopoulou, Angelopoulos, et al., 2017; Fernandes et al., 2018; Hatamian, 2020; Kounoudes & Kapitsaki, 2020; Masmoudi et al., 2018; Morel et al., 2019; Pedrosa et al., 2019)
Log when sensitive information is being accessed and processed	(Badii et al., 2020; Colesky & Ghanavati, 2016; Gonçalves et al., 2020; Hjerppe et al., 2019; Morales-Trujillo & Garcia-Mireles, 2018; Rhahla et al., 2021)

Minimize.

This is the most straightforward strategy. The less data you collect, the less the risk associated with processing and storing such data. The amount of data collected and processed should be reduced to the minimum possible. This should be decided on a case-by-case basis (Colesky & Ghanavati, 2016; Kung et al., 2017) and possibly limited to only data required for the functionality of the application (Abdulghani et al., 2019; Hatamian, 2020). According to this strategy, irrelevant information should be removed from the user's representation (Morales-Trujillo & Garcia-Mireles, 2018) by stripping off relevant and privacy-sensitive meta-data (Colesky & Ghanavati, 2016). Minimizing storage retention also helps in reducing the risk associated with data breaches (Abdulghani et al., 2019), as having data stored only for a limited time will reduce the impacts of a violation.

Separate.

Data breaches can also be mitigated by adopting separate strategies. Separate means splitting data across different hardware (physical separation) or splitting data on a software level (logical separation) (Gabel & Schiering, 2019). A possible separate strategy involves dividing users' data into sub-profiles (fragments) belonging to the same identity (Gabel & Schiering, 2019), which are assigned to different pseudonyms that only authorized users know. Another solution could be cross-domain unlinkability, which aims at separating data and processes so that processes are operated in a way that makes data unlinkable to other privacy-relevant information outside the domain (Mougiakou & Virvou, 2017). Decentralized storage (Abdulghani et al., 2019; Custers et al., 2018) (e.g., distributed-based storage with proper encryption), isolation and virtualization (Colesky & Ghanavati, 2016; Kung et al., 2017) (e.g., through application containerization), and system interconnection via overlay networks or message brokers are also suggested (Coroller et al., 2018; Pedrosa et al., 2019). To this end, (Coroller et al., 2018) propose an architecture to provide end-to-end data control in event-based systems considering GDPR requirements on consent and data processing. Model View Controller (MVC) architectures also support this strategy by separating the data (model) from the UI (view), allowing for better management, at the data level, of what data is shown to the user (Morales-Trujillo & Garcia-Mireles, 2018).

Abstract.

Abstract means to adopt techniques to look at the data from a more general point of view to minimize the privacy risk for single individuals. Usually, when processing data, the final aim is to find a general rule to guide our decisions. Thus, we do not need to go deeply into processing the data of a single individual. Still, we may achieve similar results (and not necessarily less accurate) by considering data from groups of people with similar characteristics. Different solutions are discussed under the abstract strategy, including *a)* homomorphic encryption (Abdulghani et al., 2019), which allows performing computation over encrypted data;

b) differential privacy (Sokolovska & Kocarev, 2018), which allows querying a dataset in a privacy-preserving way; *c)* k-anonymity, and its extensions l-diversity, t-closeness (Gruschka et al., 2018), which are anonymization techniques that ensure that is not possible to identify single records in a specific dataset (a dataset is said to be k-anonymous if a record cannot be distinguished from a minimum of k-1 other records present in the dataset).

Data aggregation over time (Mannhardt et al., 2018) and privacy-aware data-analysis algorithms (e.g., according to Statistical Disclosure Limitation – SDL techniques and/or randomized response methods (Sokolovska & Kocarev, 2018)) are also suggested. Derivation, which means replacing detailed information with equivalent but more general ones (e.g., substitute data of birth with age) and approximation (replacing information with less specific one) are also valid techniques to implement this strategy (Saatci & Gunal, 2019).

Hide.

The hide strategy asks for the confidentiality of data, meaning that data should be protected and not disclosed to any unauthorized party. Confidentiality is, of course, guaranteed by implementing encryption mechanisms, which is always recommended both for storage and transfer (Mougiakou & Virvou, 2017) (one should also consider the possibility to put the user in control, by exploiting client-side encryption (Mannhardt et al., 2018)). Indeed, it is always recommended to run application layer protocols over Transport Layer Security (TLS) (C. Li & Palanisamy, 2019). Attribute-Based Encryption (ABE) (Coroller et al., 2018), an asymmetric encryption technique that allows encrypting data according to attributes that describe the user, is suggested as a method to easily provide both confidentiality and access control in a scalable way without the need for complex security infrastructures. With ABE, only users with specific attributes can decrypt the encrypted information.

Masking (hiding part of the data), Mixing (mixing data from multiple records), and Tokenization (replacing data with unique ids) are also suggested as ways to implement this strategy (Saatci & Gunal, 2019). Finally, logging should always be carefully performed to avoid disclosing plain-text sensitive data in logs (Papageorgiou et al., 2018).

Inform.

The explanation is a critical process for this strategy. Users must take an informed decision about their data. Indeed, users should always be explained the whole personal data process in a detailed but understandable and concise way (Colesky & Ghanavati, 2016), including any data collection and sharing that is taking place (Hatamian, 2020) and, eventually, how data from different sources is combined, and for what and for how long data will be stored (Mannhardt et al., 2018). Moreover, a list of third parties to which data may be forwarded should be provided (Butin & Le Métayer, 2015), and any other policy update must be notified to the user (Mohan et al., 2019). Furthermore, as explicitly mandated by the different privacy regulations, data breaches must be notified “without undue delay” (Ataei et al., 2018) and specifically within 72 hours from the identification of the breach, according to the GDPR.

The consequences of not providing data should also be explained (Ataei et al., 2018; Betzing et al., 2019), together with explaining the difference between what data is necessary and what data can be voluntarily shared (Wachter, 2018b). In any case, the process of asking for users' consent must be separated from the choice of enabling other service-related features (Colesky & Ghanavati, 2016; Hatamian, 2020).

Many authors agree that visual reminders could support this strategy (Ataei et al., 2018). To this end, a methodology to generate machine-readable privacy icons is proposed in (Palmirani et al., 2018). It consists of analysing and formalising legal requirements into an ontology and generating the related pictorial representations through a participatory multidisciplinary design workshop. The designed icons are then empirically assessed according to an association test to evaluate the ability of the users to recognise icons for their legal meaning.

However, some authors state also that icons might not always be the best tool for communication (Wachter, 2018a): even if the short descriptive text accompanies them, they cannot be enough to explain the complexity of some automated decision-making processing as requested by the regulations; thus other solutions need to be defined.

Finally, Transparency Enhancing Tools (TET) (Spagnuelo et al., 2019), which support users in gaining more knowledge about their data, can help pursue this strategy.

Control.

Control means empowering users with ways to exercise their rights. This strategy should be implemented by adopting user-centric approaches, meaning that users should have complete control over the data they want to share and how they want to share them, but without being overwhelmed by the complexity of the process. This could be supported, for example, by automating part of the process (C. Li & Palanisamy, 2019). As Morel et al. suggest, control should also be implemented in a way that minimizes fatigue while maximizing the likelihood for the user to make the appropriate decision (Morel et al., 2019). This can be enabled, for example, by a privacy dashboard (Kung et al., 2017), or by supporting users' decisions by using machine-readable policy formats (Martucci et al., 2017; Pardo & Le Métayer, 2019). In any case, users should be able to continually access and update collected data and remove them from the collection (Ataei et al., 2018). To this end, in the context of the Internet of Things (IoT), Wachter states that “disconnect” features for smart devices should also be implemented (Wachter, 2018a), allowing to disable at any time the networking functionality of IoT devices to safeguard users’ privacy. Eventually, users could also be allowed to specify how long data can be stored and used (Mannhardt et al., 2018).

A relevant user-oriented solution worth mentioning is defined as “Sticky Policies”, where users can define a set of rules that specifies how service providers shall handle the data they are sharing (Kung et al., 2017). However, this solution presents a few shortcomings: on the one hand, Sticky Policies are not easy to be used by all users (specifically less expert ones), on the other hand, they are too generic and not service-specific, thus resulting in being less effective (Gol Mohammadi et al., 2019). Gol Mohammadi et al. address these issues by extending the sticky policies concept. They propose a user-oriented framework where users can define their privacy preferences for a specific service in a user-friendlier way, structure information about data processing in a tabular way (instead of the textual privacy policy), and reuse their preferences for any future policy negotiation with other services (Gol Mohammadi et al., 2019).

A promising approach for fostering control is MyData (Su et al., 2016), a user-centric framework to facilitate personal data sharing in a controlled flow, enabling users to control where their data goes, define who can use them and modify these decisions over time.

In any case, service providers should move away from a take it or leave it to approach (Gol Mohammadi et al., 2019), meaning that users should not be forced to agree with the privacy policy to use the service completely, but should be left with the choice of their preferred balance between functionality and privacy (Custers et al., 2018). All of this should be provided in an agile fashion (Wachter, 2018a), allowing informed tailoring and management of privacy preferences. In addition, service providers should clearly distinguish between data required for service functionalities and optional data that can be voluntarily shared (Wachter, 2018b). It is worth mentioning that the studies reported in (Hatamian, 2020) and (Abdulghani et al., 2019) suggest that, in any case, only data exclusively required for the proper functionality of the service should be collected according to the minimize strategy.

Enforce.

This strategy includes more procedural solutions rather than pure technical solutions, supporting a methodological approach to enforce privacy compliance at a business level. Enforce means getting in the mindset of ensuring regulatory compliance. This is why it is worth highlighting how educating the development team (Ataei et al., 2018; Campanile et al., 2022) as well as the end-users (Custers et al., 2018) is considered crucial to make this strategy (and the other 7) effective. In this regard, Diamantopoulou et al. suggest specific actions to be taken to increase employees' information security awareness through training and disciplinary processes (Diamantopoulou et al., 2020). Indeed, education has always been a pillar of usable security and privacy (Cranor & Garfinkel, 2005). Nevertheless, educating, especially the end user, is an ambitious and challenging task.

Different solutions propose models that help in complying with various privacy requirements. Martin et al. highlight how developers are unprepared to deal with privacy requirements and lack the tools (and the methods) to translate those requirements into the software. Thus, they suggest adopting a model-driven design to support engineers with GDPR-compliant software development (Martin & Kung, 2018). Similarly, (Fatema et al., 2017) propose a data management model to make consent specific and unambiguous, enabling GDPR-compliant data processing. Moreover, in (Alshammari & Simpson, 2017a), a UML-based data lifecycle model is proposed. Different privacy principles are represented as requirements, and constraints provide the criteria to assess whether the representation of the data processing fulfils the requirements, facilitating the modelling of the data lifecycle and the adoption of different principles, such as the separation of duties and data minimisation. In (Ahmadian, Strüber, et al., 2018), Ahmadian et al. present a privacy-aware system design model to mitigate possible regulation violations during the design process. This is enabled by building on top of existing Privacy Impact Assessment (PIA) methods to identify risks, proposing, through a cost-benefit approach, a set of reusable components that can be practically implemented to mitigate those risks. Furthermore, in (Bartolini et al., 2015), an ontology-based business process methodology to address GDPR requirements is presented to support data controllers in complying with the regulation, auditors to assess compliance, and the authorities to detect potential violations.

To implement this strategy, the *10 Global Privacy Standard* principles (Cavoukian, 2006) should always be considered to support the effective development of privacy-aware solutions (Alshammari & Simpson, 2017c). Once the requirements are implemented, a process should be set up to regularly assess, test, and validate the effectiveness of the implemented measures (Morales-Trujillo & Garcia-Mireles, 2018). Such a process can also be automated (Agarwal et al., 2018) to improve its effectiveness and continuously verify these requirements.

It is fundamental that, in any case, data should be collected if and only if the user has given consent (Antignac et al., 2018). To this end, to adhere to the privacy-by-default strategy, the least privacy-invasive choice should be selected for the user by default (Mustafa et al., 2019), and the user must be able to withdraw the consent at any time (Fernandes et al., 2018).

Demonstrate.

The demonstrate strategy is strictly related to the enforce strategy. Once we understand that we need to comply with the principles and we define the methods and the processes to do so, we also need a way to demonstrate, for example, to the authorities, that we are correctly complying with the regulation. As a first consideration, we can say that adopting documented methods and management procedures (Martin & Kung, 2018) supports the demonstrate strategy enabling compliance verification and transparency. To this end, logging is also important to keep Records of Processing Activities (ROPA) as requested by article 30 of the GDPR, by article 37 of the LGDP, and similarly required by the California Privacy Laws (Diamantopoulou, Angelopoulos, et al., 2017). Indeed, logging should always be performed when the user consents to the processing and when accessing, processing, updating and deleting personal data (Hjerppe et al., 2019). Accordingly, a record of users' consent decisions should also be maintained (Butin & Le Métayer, 2015) to decide the accountability of any decision (Pedrosa et al., 2019).

Most authors seem to agree that performing a Data Protection Impact Assessment (DPIA), even in that cases that are not mandatory, such as for the PIPEDA, LGDP, and California Privacy Laws and only under certain circumstances of the GDPR, can help to comply with the regulations as the DPIA is considered a powerful self-assessment tool (Coles et al., 2018). To this end, adopting data lifecycle models (Alshammari & Simpson, 2017a) can also help identify critical tasks and risks in the data management process (Alshammari & Simpson, 2017c).

In (Ujcich et al., 2018) the authors propose a data provenance model composed of different patterns (i.e., data collection and consent by a subject, data transfer among controllers and processors, withdrawal by a subject), for representing GDPR workflows to support reasoning on how data are collected and processed.

How Privacy-By-Design and Privacy-By-Default principles integrate into an HCD process? (RQ2)

To analyze the 29 publications selected for RQ2 we identified 3 dimensions summarized by the following questions:

- What are the HCI methodologies adopted to comply with privacy?
- What are the challenges in adopting such measures?
- Are there any gaps in the current technologies?

Answering such questions can help identify how these privacy principles relate to HCI methodologies nowadays. The complete list of solutions that answer such questions is reported in Table 2. In the following, the three points of view are described, and some representative articles are discussed.

Table 2. Results of the data extraction for RQ2

What are the HCI methodologies adopted to comply with privacy requirements?	
Requirements Phase	
Reach Universal Usability	(O'Connor et al., 2017)
Design Phase	
Value-centered design, Redesign and future envisioning approaches	(Muller & Lévy, 2019; Perera et al., 2021; Schnädelbach et al., 2019; Wong & Mulligan, 2019)
User-Centered Design (UCD)	(Jakobi et al., 2019; Urquhart, 2016)
Development Phase	
Implementation Security and Privacy HCI patterns	(Loruenser et al., 2018)
Evaluation Phase	
A/B testing	(Ayalon & Toch, 2019)
User Study	(Alpers et al., 2017; Karegar et al., 2018)
What are the challenges in adopting such measures?	
Privacy solutions can be subjective and sensitive to sociocultural differences	(Ayalon & Toch, 2021; Barbosa et al., 2020; Ceross & Simpson, 2018; Wong & Mulligan, 2019)
UX designers are not involved in privacy efforts	(Alkhatib et al., 2020; Ceross & Simpson, 2018; Rossi & Lenzini, 2020; Wong & Mulligan, 2019)
The system functionalities and legal implications must be fully understood by all stakeholders of the solution	(Alhazmi & Arachchilage, 2021; Alkhatib et al., 2020; Barbosa et al., 2020; Gkotsopoulou et al., 2019; Jakobi et al., 2019; Kühtreiber et al., 2022; Loruenser et al., 2018; Mangini et al., 2020)
Technology variety and complexity, user diversity and gaps in user knowledge	(Bowyer et al., 2022; O'Connor et al., 2017; Urquhart, 2016; Wright, 2019)
Are there any gaps in the current technologies?	
There is less focus on ensuring usable privacy rather than pure technical privacy measures	(Alkhatib et al., 2020; Alpers et al., 2017; Bernabe et al., 2019; Bowyer et al., 2022; Jakobi et al., 2019)
Users are happier to skip the interaction rather than setting up their privacy preferences (Hyperbolic discounting)	(Kounoudes & Kapitsaki, 2020; Rossi & Lenzini, 2020; Urquhart, 2016)
It can be unclear to users what information can be extracted from the variety and vast volume of data collected	(Jakobi et al., 2019; O'Connor et al., 2017)
Legal frameworks and standards need to be accompanied by methodologies to help software engineers during the development process	(Alshammari & Simpson, 2018; Ataei et al., 2018; Tahaei et al., 2021; Veale et al., 2018)

What are the HCI methodologies adopted to comply with privacy?

To comply with privacy, several HCI methodologies can be applied during the different phases of the software lifecycle, namely requirement collection and analysis, design, development and evaluation.

Regarding the *requirement* phase, the system should aim at reaching the so-called universal usability (Shneiderman, 2000), a concept introduced by Ben Shneiderman according to which a system should be designed to be usable for all individuals, enabling them to succeed in their tasks while interacting with the system.

In the *design* phase, this requirement can be satisfied by defining new roles in the teams, explicitly including UX designers in privacy efforts, and using value-centered design, re-design and speculative and critical design approaches (Wong & Mulligan, 2019). These approaches aim to solve privacy problems and widen our understanding of privacy as a socio-technical concept and what it entails for people, allowing us to design future-proof privacy solutions. As an example, Schnädelbach et al. (Schnädelbach et al., 2019) propose future envisioning to design privacy-aware adaptive architecture highlighting the design tensions between smart buildings and privacy requirements. Urquhart et al. (Urquhart et al., 2018) suggest adopting design ethnography as well as co-design approaches to better respond to users' needs in terms of privacy. Indeed, the users are still not considered enough during the design of security and privacy features (Ayalon & Toch, 2021), and these methodologies can help involve the users in the design process itself.

To this end, during the *development* phase, security and privacy-HCI patterns (Länger et al., 2018) can be adopted to support the usable implementation of security and privacy mechanisms. However, the reference catalogue is still quite restricted, and more research has to be done to strengthen and extend the proposed patterns.

During the *evaluation* phase, user studies are effectively adopted to evaluate privacy interfaces (Alpers et al., 2017) and if users make informed decisions during the consent process (Karegar et al., 2018). Ayalon et al. (Ayalon & Toch, 2019) use A/B testing to support researchers and decision-makers in designing and evaluating privacy solutions by proposing a *perceived privacy scale* to assess users' perceptions concerning the different designs that they are presented to. Nevertheless, evaluating the technology mechanism developed for complying with privacy requirements is critical to ensure that the proposed solutions also meet users' privacy expectations (Ayalon & Toch, 2019).

What are the challenges in adopting such measures?

The publications analysed led us to identify different shortcomings in the design of privacy-compliant systems. First, a problem that Wong et al. identified is that privacy is sensitive to sociocultural differences (Wong & Mulligan, 2019) and subjective (Ceross & Simpson, 2018). Thus, user diversity, as well as gaps in user knowledge, are identified as a problem to reach universal usability (Shneiderman, 2000). Users have different perspectives on privacy: some may be more willing to share their data online, while others may feel uncomfortable doing so and prefer not to share any data at all. While users seem to be quite pleased by the new and more strict privacy regulations, they mistrust the companies processing their data. Thus, more work has to be done to provide more control to users (Bowyer et al., 2022) while ensuring that their privacy is preserved and they understand the implications and risks involved in sharing their data, as this may be not always clear (Jakobi et al., 2019).

Indeed, privacy is not an easy concept. It may be not easy to understand not only for users (Jakobi et al., 2019) but also for developers (Barbosa et al., 2020), who must understand both the technical and the theoretical side of this field (Loruenser et al., 2018). In this sense, HCI experts are still not involved enough in the development process of privacy solutions (Wong & Mulligan, 2019), which instead is recognized as critical (Rossi & Lenzini, 2020) to make these solutions usable, by linking together the user experience, regulatory compliance, and system requirements (Ceross & Simpson, 2018).

Are there any gaps in the current technologies and approaches?

As privacy regulations start embracing the user-centric approach (Sobolewski et al., 2017), it is clear that a lot needs to be done in this sense. There is more focus on pure technical measures rather than usability aspects (Jakobi et al., 2019), which are often overlooked (Alpers et al., 2017) and, to this end, there is a lack of comprehensive approaches for usable privacy (Bernabe et al., 2019). Alkhatib et al. state that users feel the importance and need for privacy, but this is neglected by implementing the privacy-by-design principle in practice (Alkhatib et al., 2020). These poor designs negatively impact users (Kounoudes & Kapitsaki, 2020) as often they fail to be informed and blindly agree to the terms (Rossi & Lenzini, 2020). To this end, Urquahart refers to hyperbolic discounting: users are happier to skip the interaction rather than to set their privacy preferences. This problem becomes more and more prominent as technology evolves and specifically when we consider the heterogeneity of IoT technologies (Urquhart et al., 2018) and complex solutions (e.g., blockchain (Wright, 2019)). Since even developers can struggle with following guidelines, and this can be attributed to the complexity of the regulations and their level of abstraction (Ataei et al., 2018), there is a strong need to accompany legal frameworks and standards with methodologies that ease the development process of privacy solution (Veale et al., 2018). Indeed, while the privacy-by-design paradigm represents a step forward in this direction, there are still challenges to be addressed as the generality of these principles hinders their practical implementation (Alshammari & Simpson, 2018).

The above discussion identified major shortcomings regarding the privacy requirements implementation from a usability point of view, implying that there is still room for significant improvements. In this sense, the next section proposes some inputs for researchers to fill out the highlighted gaps. The following discussion focuses specifically on the GDPR since, as previously said, it is currently the most advanced privacy regulation.

How can the proposed framework be used in real scenarios?

This SLR answered the two RQs by defining a framework reporting a set of solutions that different stakeholders can use during the different phases of the software development lifecycle. To better illustrate and clarify how this framework can be adopted in real contexts, we present below some scenarios for using the results of this SLR.

Development of the Website for an Italian Public Administration

The Municipality of Rome has decided to develop its new website to provide citizens and tourists with all the necessary information and current services. The development was entrusted to the company Software4PA Spa. Among the various requirements the company has to satisfy, one of the most important is website compliance with the GPDR, a mandatory prerequisite for all Italian public administrations. In particular, they have to consider what is indicated in article 25, which requires guaranteeing security and privacy "by design" and "by default". To speed up its development, avoid misinterpretations of the GPDR by its engineers and ensure a high quality of the software components that meet this requirement, the project manager of Software4PA decided to use the framework proposed in this paper. She started by examining the solutions reported in Table I, one strategy at a time, and selected a list of requirements. For example, for the 'Minimise' strategy, she decided that a critical aspect is the data collection, which needs to be minimised to what is required for the application to function properly and to show the website users the data that is strictly necessary to avoid unnecessary disclosure. As another example, for the "Hide" strategy, she decided that the website must implement encryption both for transmission (TLS protocol) and storage and avoid logging sensitive information as personal data. In the end, the engineer reports the requirements in a document for the software designers, who can follow such prescriptions to ensure security and privacy 'by design' and 'by default' in the website in the next phases of the software lifecycle.

Reingengnerization of a Public administration system.

Company LMOStars Srl was commissioned to re-engineer the territorial registry system used by the Apulia Region because of the introduction of national and supranational data privacy laws. This system processes the personal data of around one million users, and the two main functionalities are data collection and validation of citizens. The reengineering required introducing privacy and security requirements, as the system had been subject to data exfiltration. In particular, to integrate the principles of Privacy by Design and by Default and to be GDPR compliant, the development team was supported by the framework proposed in this study for the requirements analysis and design phase. Specifically, to reduce the exposure of personally identifiable information (PII) and threat agents by examining the privacy design strategies identified in Table I, the team was operationally supported in mapping the privacy vulnerabilities identified during static and dynamic code analysis with the appropriate strategies. Different strategies were selected from the framework when analysing the vulnerabilities with critical priority (injection, broken authentication, sensitive data exposure, security misconfiguration, cross-site scripting). First, "Minimise" was chosen to limit data collection to what is required for the proper functioning of the application, minimise the retention of data to reduce the risks associated with data breaches, carefully select the data to be processed. "Separate" to process data in a distributed manner through isolation and virtualisation and to separate user data into sub-profiles; ensure cross-domain inviolability through context separation. "Hide" to use encryption at rest and in transit and to hide sensitive data through masking, blending and tokenisation. "Inform" to explain the process of processing personal data in a detailed, concise and understandable way; asking for a user's consent to process their personal data must be separated from asking for consent to services offered. "Control" to enable users to learn and exercise their rights (access, rectification, erasure, giving and withdrawing consent and portability) through the system UI/dashboard. "Enforce" to adopt ontologies to model information related to personal data to improve interpretation, visualisation and compliance checking against privacy policies.

Development of a mobile app for diet following a User-Centred Design.

Healthy Food Ltd is a UK company whose core business is developing software to help people eat healthily. Recognising the growing trend towards using mobile applications, they decided to develop a new mobile application that would generate a diet plan based on the user's profile and needs. Two critical aspects of this project are the collection of sensitive data, which requires a lot of attention to privacy and usability. Based on the framework proposed in this study, they followed an HCD process to ensure high usability and privacy. Apart from following the prescription reported in the previous scenarios to design and develop the user interface and user interaction, they carefully followed the suggestions that the framework reported in the four phases, i.e., requirements, design, development and evaluation. For example, as suggested in the requirements phase, they wanted to develop a system that everyone would use, enabling them to complete their tasks while interacting with the system successfully. To this end, they decided to identify all the potential target users, interview them to gather requirements and identify the specific needs of each type of user. Then, in order to design the application, as suggested by the framework, as a specific process for HCD, they adopted ISO 9241:2020. They also decided to include UX designers for privacy aspects in their team. Then, in both the design and development phases, they considered a catalogue of privacy HCI patterns to facilitate the implementation of usable security and privacy mechanisms. Finally, the developed application was also evaluated through user studies, focusing on traditional usability aspects and privacy issues, for example, when users make informed decisions during the consent process.

Further Research Directions

The analysis of the results of the RQs reported several solutions and technologies that address different approaches to privacy-by-design and privacy-by-default for privacy-compliant software development. In the following, we sum up further research directions that should be critical for future work to build on.

Support engineers during the development process

Implementing security mechanisms is not an easy task. Moreover, there is often a need for a deep understating of the architectures and the technologies involved in the solutions (Alhazmi & Arachchilage, 2021; Gkotsopoulou et al., 2019; Hadar et al., 2018). Furthermore, some authors have highlighted a general lack of preparation in terms of security and privacy knowledge from developers (Barbosa et al., 2020; Lodge & Crabtree, 2019; Martin & Kung, 2018). This makes designing and developing secure and compliant software even more difficult. To this end, there is a need, for security training for software engineers to increase their awareness about security and privacy risks associated with the digital ecosystem and then to ease their work by providing more strict but practical methodologies and procedures to guide the development process (Alshammari & Simpson, 2017c; Veale et al., 2018), as it was highlighted that developers still struggle even with following the guidelines (Ataei et al., 2018; Barbosa et al., 2020).

Make compliance user-centered

It is fundamental to understand that compliance is not only a critical step but a mandatory one. In this sense, the most effective way to comply with this obligation is by considering privacy from the ground up, i.e., privacy-by-design (and, thus, compliance-by-design). The requirements mapped in the 8 privacy design strategies provided by this work will help further ease developers with more practical pointers for implementing such strategies according to the privacy-by-design principles and under the different regulatory requirements. However, most of the publications analyzed for RQ1 do not provide any consideration from an HCI point of view. This means that, even if we find out that multiple solutions can be implemented to ensure compliance, they may not be usable and so not be well received by end users (Alpers et al., 2017; Bowyer et al., 2022). Since the privacy principles claim to put at the centre the final users, it is conflicting that the technological implementations of these processes lack a deeper understanding of the users' perspective.

Foster usable privacy implementations

While the GDPR sets itself as a user-centric regulation and the other regulations are following up, their technological implementations are not. The results of RQ2 further corroborate this view. Not only there is less research interest from the usable-privacy point of view, as can be observed by the lower number of publications retrieved, but most of the works in this field confirm that these issues are still not tackled enough or at all by the privacy-engineering community (Bernabe et al., 2019). Indeed, in (Jakobi et al., 2019), it is highlighted how privacy-by-design guidelines are focused more on the technological point of view, while users often are not considered in such processes.

Wong and Mulligan (Wong & Mulligan, 2019) suggest how HCI and privacy communities should work hand in hand to improve privacy-by-design research and practice, as usability is frequently overlooked in privacy solutions (Alpers et al., 2017). In (Loruenser et al., 2018), the authors highlight that applying HCI patterns is vital to seamlessly embed both requirements and domain knowledge so that information can be accessed and properly handled by all involved actors independently from their actual technical background. Moreover, as Kounoudes et al. point out, usable user interfaces, the process of informed consent and possible context-aware user privacy preferences are still open research issues (Kounoudes & Kapitsaki, 2020).

To this end, we can say that more impactful methodologies are required to ease the process of integrating privacy and HCI patterns, or even the definition of new usable privacy patterns may be needed to address the issue and meet at the same time both the users' expectations and regulatory requirements.

Guarantee transparency and trustworthiness for a "win-win" scenario

Putting the user in control of their data is not enough. There is a need for solutions that guide the users and ease their interaction process of informed consent (Urquhart, 2016). To this end, there is also a need for comprehensive campaigns to increase users' privacy awareness (Kounoudes & Kapitsaki, 2020). Users should have the knowledge and the freedom to choose their preferred settings when sharing data with third-party services (Bowyer et al., 2022). This should possibly result in a win-win situation both for users and service providers: on the one hand, users are educated, aware, and informed on the data collection and their processing and understand the involved risks. On the other hand, once understand the rationale behind the data being collected and their purposes, possibly in a transparent and trustworthy manner, users may be more inclined to share data with service providers that will indeed benefit from the acquired data.

Conclusion and Future Work

This study addressed the challenges and open issues of translating data privacy regulations into software requirements. A systematic literature review was conducted to identify a set of software requirements and business processes for Privacy-By-Design and Privacy-By-Default, as well as HCI methodologies used to meet privacy requirements. The results of this study allowed the definition of an initial framework whose adoption will benefit software engineers, designers and developers by accelerating the translation of such principles into software requirements, improving the quality of software development, and avoiding misinterpretations. In addition, this framework can help developers to implement more user-centric software requirements, even if they lack expertise in HCI, as the proposed mapping guides the most effective HCI solutions for different stages of software development. The identified solutions provide many tools, methodologies, and solutions for use according to the specific strategy and use cases to support privacy-aware software implementation.

The proposed framework provides more concreteness to the principles of Privacy-By-Design and Privacy-By-Default. However, several aspects must be further developed to provide stakeholders with a more concrete and broader methodological toolkit. For example, the requirements in Table I and Table II represent valid and concrete solutions, but more practical approaches could be identified. For instance, starting from this strategy and the GDPR article, we have already begun investigating privacy design patterns that drive coding activities and user interface design (Barletta et al., 2022).

Still, the analysis showed that, while from a technological point of view, many different solutions exist to support regulatory requirements implementation on different levels effectively, there is still a lot to be done to make these tools and methods more user-centred.

As further future works, we also highlighted the need to include in developers' security training and guidelines to support their job. Shortly, close cooperation between HCI and security/privacy experts is expected to ease the adoption of privacy-enhancing technologies and strategies that meet, at the same time, both users' privacy expectations and business objectives. As a result, since the development of security features has often overlooked the principles of usability and human-computer interaction in general, a future goal of this work is to propose a comprehensive and practical technical and methodological framework to support the user-centric design of regulatory-compliant software.

References

Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective. *Symmetry*, *11*(6), Article 6. https://doi.org/10.3390/sym11060774

Agarwal, S., Steyskal, S., Antunovic, F., & Kirrane, S. (2018). Legislative compliance assessment: Framework, model and GDPR instantiation. *Annual Privacy Forum*, 131–149.

Agostinelli, S., Maggi, F. M., Marrella, A., & Sapio, F. (2019). Achieving GDPR compliance of BPMN process models. *Lecture Notes in Business Information Processing*, *350*, 10–22. https://doi.org/10.1007/978-3-030-21297-1_2

Ahmadian, A. S., Jürjens, J., & Strüber, D. (2018). Extending Model-Based Privacy Analysis for the Industrial Data Space by Exploiting Privacy Level Agreements. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1142–1149. https://doi.org/10.1145/3167132.3167256

Ahmadian, A. S., Strüber, D., & Jürjens, J. (2019). Privacy-Enhanced System Design Modeling Based on Privacy Features. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 1492–1499. https://doi.org/10.1145/3297280.3297431

Ahmadian, A. S., Strüber, D., Riediger, V., & Jürjens, J. (2018). Supporting Privacy Impact Assessment by Model-Based Privacy Analysis. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1467–1474. https://doi.org/10.1145/3167132.3167288

Alhazmi, A., & Arachchilage, N. A. G. (2021). I'm all ears! Listening to software developers on putting GDPR principles into software development practice. *Personal and Ubiquitous Computing*, *25*(5), 879–892. https://doi.org/10.1007/s00779-021-01544-1

Alkhatib, S., Waycott, J., Buchanan, G., Grobler, M., & Wang, S. (2020). Privacy by Design in Aged Care Monitoring Devices? Well, Not Quite Yet! *Proceedings of the 32nd Australian Conference on Human-Computer Interaction*, 492–505. https://doi.org/10.1145/3441000.3441049

Al-Momani, A., Kargl, F., Schmidt, R., Kung, A., & Bösch, C. (2019). A Privacy-Aware V-Model for Software Development. *2019 IEEE Security and Privacy Workshops (SPW)*, 100–104. https://doi.org/10.1109/SPW.2019.00028

Alpers, S., Oberweis, A., Pieper, M., Betz, S., Fritsch, A., Schiefer, G., & Wagner, M. (2017). PRIVACY-AVARE: An approach to manage and distribute privacy settings. *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, 1460–1468. https://doi.org/10.1109/CompComm.2017.8322784

Alshammari, M., & Simpson, A. (2017a). A UML profile for privacy-aware data lifecycle models. In *Computer Security* (pp. 189–209). Springer.

Alshammari, M., & Simpson, A. (2017b). *Personal Data Management for Privacy Engineering: An Abstract Personal Data Lifecycle Model*. Oxford, UK, CS-RR-17-02.

Alshammari, M., & Simpson, A. (2017c). Towards a principled approach for engineering privacy by design. *Annual Privacy Forum*, 161–177.

Alshammari, M., & Simpson, A. (2018). Privacy Architectural Strategies: An Approach for Achieving Various Levels of Privacy Protection. *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, 143–154. https://doi.org/10.1145/3267323.3268957

Antignac, T., Scandariato, R., & Schneider, G. (2018). Privacy Compliance Via Model Transformations. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 120–126. https://doi.org/10.1109/EuroSPW.2018.00024

Ataei, M., Degbelo, A., Kray, C., & Santos, V. (2018). Complying with privacy legislation: From legal text to implementation of privacy-aware location-based services. *ISPRS International Journal of Geo-Information*, *7*(11), Article 11.

Ayala-Rivera, V., & Pasquale, L. (2018). The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements. *2018 IEEE 26th International Requirements Engineering Conference (RE)*, 136–146. https://doi.org/10.1109/RE.2018.00023

Ayalon, O., & Toch, E. (2019). A/P(Rivacy) Testing: Assessing Applications for Social and Institutional Privacy. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3290607.3312972

Ayalon, O., & Toch, E. (2021). User-centered privacy-by-design: Evaluating the appropriateness of design prototypes. *International Journal of Human-Computer Studies*, *154*, 102641.

Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. *IEEE Access*, *8*, 23601–23623. https://doi.org/10.1109/ACCESS.2020.2968741

Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2020). Integrating security and privacy in software development. *Software Quality Journal*, *28*(3), 987–1018. https://doi.org/10.1007/s11219-020-09501-6

Barbosa, P., Brito, A., & Almeida, H. (2020). Privacy by Evidence: A Methodology to develop privacy-friendly software applications. *Information Sciences*, *527*, 294–310.

Barletta, V., Desolda, G., Gigante, D., Lanzilotti, R., & Saltarella, M. (2022). From GDPR to Privacy Design Patterns: The MATERIALIST Framework. *Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT,* 642–648. https://doi.org/10.5220/0011305900003283

Bartolini, C., Muthuri, R., & Santos, C. (2015). Using ontologies to model data protection requirements in workflows. *JSAI International Symposium on Artificial Intelligence*, 233–248.

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, *7*, 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872

Besik, S. I., & Freytag, J.-C. (2019). A formal approach to build privacy-awareness into clinical workflows. *Software-Intensive Cyber-Physical Systems*. https://doi.org/10.1007/s00450-019-00418-5

Betzing, J. H., Tietz, M., vom Brocke, J., & Becker, J. (2019). The impact of transparency on mobile privacy decision making. *Electronic Markets*, 1–19.

Bowyer, A., Holt, J., Go Jefferies, J., Wilson, R., Kirk, D., & David Smeddinck, J. (2022). Human-GDPR Interaction: Practical Experiences of Accessing Personal Data.

Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3491102.3501947

Butin, D., & Le Métayer, D. (2015). A Guide to End-to-End Privacy Accountability. *Proceedings of the First International Workshop on TEchnical and LEgal Aspects of Data PRIvacy*, 20–25.

Caiza, J. C., Martín, Y., Guamán, D. S., Alamo, J. M. D., & Yelmo, J. C. (2019). Reusable Elements for the Systematic Design of Privacy-Friendly Information Systems: A Mapping Study. *IEEE Access*, *7*, 66512–66535. https://doi.org/10.1109/ACCESS.2019.2918003

Campanile, L., Iacono, M., & Mastroianni, M. (2022). Towards privacy-aware software design in small and medium enterprises. *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 1–8. https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927958

Canadian Standing Committee on Access to Information, Privacy and Ethics. (2018). *Towards privacy by design: Review of the personal information protection and electronic documents act*. https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf

Cavoukian, A. (2006). Creation of a Global Privacy Standard. *Published November*, *8*.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and privacy commissioner of Ontario, Canada.

Cavoukian, A., & Chanliau, M. (2013). *Privacy and security by design: A convergence of paradigms*. Information and Privacy Commissioner, Ontario.

Cavoukian, A., & Dixon, M. (2013). *Privacy and security by design: An enterprise architecture approach*. Information and Privacy Commissioner of Ontario, Canada.

Ceross, A., & Simpson, A. (2018). Rethinking the Proposition of Privacy Engineering. *Proceedings of the New Security Paradigms Workshop*, 89–102. https://doi.org/10.1145/3285002.3285006

Coles, J., Faily, S., & Ki-Aries, D. (2018). Tool-Supporting Data Protection Impact Assessments with CAIRIS. *2018 IEEE 5th International Workshop on Evolving Security Privacy Requirements Engineering (ESPRE)*, 21–27. https://doi.org/10.1109/ESPRE.2018.00010

Colesky, M., & Caiza, J. C. (2018). A System of Privacy Patterns for Informing Users: Creating a Pattern System. *Proceedings of the 23rd European Conference on Pattern Languages of Programs*. https://doi.org/10.1145/3282308.3282325

Colesky, M., & Ghanavati, S. (2016). Privacy Shielding by Design—A Strategies Case for Near-Compliance. *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, 271–275. https://doi.org/10.1109/REW.2016.051

Coroller, S., Chabridon, S., Laurent, M., Conan, D., & Leneutre, J. (2018). Position Paper: Towards End-to-End Privacy for Publish/Subscribe Architectures in the Internet of Things. *Proceedings of the 5th Workshop on Middleware and Applications for the Internet of Things*, 35–40. https://doi.org/10.1145/3286719.3286727

Cranor, L. F., & Garfinkel, S. (Eds.). (2005). *Security and usability: Designing secure systems that people can use*. O'Reilly.

Custers, B., Dechesne, F., Pieters, W., Schermer, B. W., & van der Hof, S. (2018). Consent and privacy. *Custers BHM, Dechesne F., Pieters W., Schermer B. & Hof S. van Der (2018), Consent and Privacy. In: Müller A., Schaber P.(Red.) The Routledge Handbook of the Ethics of Consent. London: Routledge*, 247–258.

Damjanovic-Behrendt, V. (2018). A Digital Twin-based Privacy Enhancement Mechanism for the Automotive Industry. *2018 International Conference on Intelligent Systems (IS)*, 272–279. https://doi.org/10.1109/IS.2018.8710526

Diamantopoulou, V., Angelopoulos, K., Pavlidis, M., & Mouratidis, H. (2017). A metamodel for GDPR-based privacy level agreements. *CEUR Workshop Proceedings*, *1979*, 299–305. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85035047124&partnerID=40&md5=69e448c703e4f4daeba149af0ee81a76

Diamantopoulou, V., Argyropoulos, N., Kalloniatis, C., & Gritzalis, S. (2017). Supporting the design of privacy-aware business processes via privacy process patterns. *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, 187–198. https://doi.org/10.1109/RCIS.2017.7956536

Diamantopoulou, V., & Karyda, M. (2022). Integrating Privacy-By-Design with Business Process Redesign. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13106 LNCS*, 127–137. https://doi.org/10.1007/978-3-030-95484-0_8

Diamantopoulou, V., & Mouratidis, H. (2019). Practical evaluation of a reference architecture for the management of privacy level agreements. *Information and Computer Security*, *26*(5), Article 5. https://doi.org/10.1108/ICS-04-2019-0052

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11980 LNCS*, 238–257. https://doi.org/10.1007/978-3-030-42048-2_16

European Network and Information Security Agency. (2014). *Privacy and data protection by design: From policy to engineering.* Publications Office. https://data.europa.eu/doi/10.2824/38623

Fatema, K., Hadziselimovic, E., Pandit, H., Debruyne, C., Lewis, D., & O'Sullivan, D. (2017). Compliance through informed consent: Semantic based consent permission and data management model. *CEUR Workshop Proceedings*, *1951*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85033485288&partnerID=40&md5=b3e538ac2a209e07a81fd0a67ac09e3b

Fernandes, M., Da Silva, A. R., & Gonçalves, A. (2018). Specification of personal data protection requirements: Analysis of legal requirements from the GDPR regulation. *ICEIS 2018 - Proceedings of the 20th International Conference on Enterprise Information Systems*, *2*, 398–405. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047745820&partnerID=40&md5=18ed86b5d55ed3a4834c66f7a0d02746

Ferrara, P., & Spoto, F. (2018). Static Analysis for GDPR Compliance. *ITASEC*.

Fritsch, L. (2017). Privacy dark patterns in identity management. *Open Identity Summit (OID), 5-6 October 2017, Karlstad, Sweden.*, 93–104.

G Karácsony, G. (2019). Managing Personal Data in a Digital Environment-Did GDPR's Concept of Informed Consent Really Give Us Control? *Počítačové Právo, UI, Ochrana*

Údajov a Najväčšie Technologické Trendy. Zborník Príspervkov z Medzinárodnej Vedeckej Konferencie. Vysoká Skola Dabubius.

Gabel, A., & Schiering, I. (2019). Privacy patterns for pseudonymity. *IFIP Advances in Information and Communication Technology*, *547*, 155–172. https://doi.org/10.1007/978-3-030-16744-8_11

Gerl, A., & Meier, B. (2019). Privacy in the Future of Integrated Health Care Services – Are Privacy Languages the Key? *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 312–317. https://doi.org/10.1109/WiMOB.2019.8923532

Gkotsopoulou, O., Charalambous, E., Limniotis, K., Quinn, P., Kavallieros, D., Sargsyan, G., Shiaeles, S., & Kolokotronis, N. (2019). Data Protection by Design for cybersecurity systems in a Smart Home environment. *2019 IEEE Conference on Network Softwarization (NetSoft)*, 101–109. https://doi.org/10.1109/NETSOFT.2019.8806694

Gol Mohammadi, N., Leicht, J., Ulfat-Bunyadi, N., & Heisel, M. (2019). Privacy Policy Specification Framework for Addressing End-Users' Privacy Requirements. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11711 LNCS*, 46–62. https://doi.org/10.1007/978-3-030-27813-7_4

Gonçalves, E., Teixeira, P., & Silva, J. P. (2020). Development of GDPR-Compliant Software: Document Management System for HR Department. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/CISTI49556.2020.9140922

Groen, E. C., & Ochs, M. (2019). CrowdRE, User Feedback and GDPR: Towards Tackling GDPR Implications with Adequate Technical and Organizational Measures in an Effort-Minimal Way. *2019 IEEE 27th International Requirements Engineering Conference Workshops (REW)*, 180–185. https://doi.org/10.1109/REW.2019.00038

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *2018 IEEE International Conference on Big Data (Big Data)*, 5027–5033. https://doi.org/10.1109/BigData.2018.8622621

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018). Privacy by designers: Software developers' privacy mindset. *Empirical Software Engineering*, *23*(1), Article 1.

Hansen, M., Jensen, M., & Rost, M. (2015). Protection Goals for Privacy Engineering. *2015 IEEE Security and Privacy Workshops*, 159–166. https://doi.org/10.1109/SPW.2015.13

Hatamian, M. (2020). Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers. *IEEE Access*, *8*, 35429–35445. https://doi.org/10.1109/ACCESS.2020.2974911

Hjerppe, K., Ruohonen, J., & Leppänen, V. (2019). The General Data Protection Regulation: Requirements, Architectures, and Constraints. *2019 IEEE 27th International Requirements Engineering Conference (RE)*, 265–275. https://doi.org/10.1109/RE.2019.00036

Hoepman, J.-H. (2014). Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Eds.), *ICT Systems Security and Privacy*

Protection (Vol. 428, pp. 446–459). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_38

Hyysalo, J., Hirvonsalo, H., Sauvola, J., & Tuoriniemi, S. (2016). Consent management architecture for secure data transactions. *ICSOFT 2016 - Proceedings of the 11th International Joint Conference on Software Technologies*, *1*, 125–132. https://doi.org/10.5220/0005941301250132

Iachello, G., & Hong, J. (2007). End-User Privacy in Human-Computer Interaction. *Foundations and Trends® in Human-Computer Interaction*, *1*(1), 1–137. https://doi.org/10.1561/1100000004

International Organization for Standardization. (2011). *Information technology—Security techniques—Privacy framework (ISO Standard No. 29100:2011)*. https://www.iso.org/standard/45123.html

Jakobi, T., Patil, S., Randall, D., Stevens, G., & Wulf, V. (2019). It Is About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. *ACM Trans. Comput.-Hum. Interact.*, *26*(1), Article 1. https://doi.org/10.1145/3281444

Karegar, F., Gerber, N., Volkamer, M., & Fischer-Hübner, S. (2018). Helping John to Make Informed Decisions on Using Social Login. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1165–1174. https://doi.org/10.1145/3167132.3167259

Kitchenham, B. A. (2004). *Procedures for Performing Systematic Reviews*.

Kneuper, R. (2020). Translating data protection into software requirements. *ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and*

Privacy, 257–264. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083031898&partnerID=40&md5=84efa030a23c2097f054006a47bc7fd9

Kounoudes, A. D., & Kapitsaki, G. M. (2020). A mapping of IoT user-centric privacy preserving approaches to the GDPR. *Internet of Things*, *11*, 100179. https://doi.org/10.1016/j.iot.2020.100179

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Trans. Web*, *15*(4). https://doi.org/10.1145/3466722

Kühtreiber, P., Pak, V., & Reinhardt, D. (2022). A survey on solutions to support developers in privacy-preserving IoT development. *Pervasive and Mobile Computing*, *85*, 101656.

Kung, A., Kargl, F., Suppan, S., Cuellar, J., Pöhls, H. C., Kapovits, A., McDonnell, N. N., & Martin, Y. S. (2017). A privacy engineering framework for the internet of things. In *Data Protection and Privacy:(In) visibilities and Infrastructures* (pp. 163–202). Springer.

Kupfersberger, V., Schaberreiter, T., & Quirchmayr, G. (2018). Security-Driven Information Flow Modelling for Component Integration in Complex Environments. *Proceedings of the 10th International Conference on Advances in Information Technology*. https://doi.org/10.1145/3291280.3291797

Kurtz, C., & Semmann, M. (2018). *Privacy by design to comply with GDPR: A review on third-party data processors*.

Ladjel, R., Anciaux, N., Pucheral, P., & Scerri, G. (2019). Trustworthy Distributed Computations on Personal Data Using Trusted Execution Environments. *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering*

(TrustCom/BigDataSE), 381–388. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00058

Länger, T., Alaqra, A., Fischer-Hübner, S., Framner, E., Pettersson, J. S., & Riemer, K. (2018). HCI Patterns for Cryptographically Equipped Cloud Services. In M. Kurosu (Ed.), *Human-Computer Interaction. Theories, Methods, and Human Issues* (Vol. 10901, pp. 567–586). Springer International Publishing. https://doi.org/10.1007/978-3-319-91238-7_44

Leite, L., dos Santos, D. R., & Almeida, F. (2022). The impact of general data protection regulation on software engineering practices. *Information and Computer Security*, *30*(1), 79–96. https://doi.org/10.1108/ICS-03-2020-0043

Lenhard, J., Fritsch, L., & Herold, S. (2017). A Literature Study on Privacy Patterns Research. *2017 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 194–201. https://doi.org/10.1109/SEAA.2017.28

Li, C., & Palanisamy, B. (2019). Privacy in Internet of Things: From Principles to Technologies. *IEEE Internet of Things Journal*, *6*(1), Article 1. https://doi.org/10.1109/JIOT.2018.2864168

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2020). GDPR Compliance in the Context of Continuous Integration. *ArXiv Preprint ArXiv:2002.06830*.

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, *146*. https://doi.org/10.1016/j.infsof.2022.106868

Lodge, T., & Crabtree, A. (2019). Privacy engineering for domestic IoT: Enabling due diligence. *Sensors (Switzerland)*, *19*(20), Article 20. https://doi.org/10.3390/s19204380

Loruenser, T., Pöhls, H. C., Sell, L., & Laenger, T. (2018). CryptSDLC: Embedding Cryptographic Engineering into Secure Software Development Lifecycle. *Proceedings of the 13th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3230833.3233765

Mangini, V., Tal, I., & Moldovan, A.-N. (2020). An Empirical Study on the Impact of GDPR and Right to Be Forgotten—Organisations and Users Perspective. *Proceedings of the 15th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3407023.3407080

Mannhardt, F., Petersen, S. A., & Oliveira, M. F. (2018). Privacy Challenges for Process Mining in Human-Centered Industrial Environments. *2018 14th International Conference on Intelligent Environments (IE)*, 64–71. https://doi.org/10.1109/IE.2018.00017

Martin, Y., & Kung, A. (2018). Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 108–111. https://doi.org/10.1109/EuroSPW.2018.00021

Martín, Y.-S., & Del Álamo, J. M. (2017). A metamodel for privacy engineering methods. *CEUR Workshop Proceedings*, *1873*, 41–48. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85027887873&partnerID=40&md5=796bc0597b45584496e3ff733aa26816

Martino, M. D., Robyns, P., Weyts, W., Quax, P., Lamotte, W., & Andries, K. (2019). Personal information leakage by abusing the GDPR "right of access." *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*, 371–386. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075610960&partnerID=40&md5=1ef23fbaa6a6d19335159b9bac4b1c4f

Martucci, L. A., Fischer-Hübner, S., Hartswood, M., & Jirotka, M. (2017). Privacy and social values in smart cities. In *Designing, Developing, and Facilitating Smart Cities* (pp. 89–107). Springer.

Masmoudi, F., Sellami, M., Loulou, M., & Kacem, A. H. (2018). Optimal Evidence Collection for Accountability in the Cloud. *2018 IEEE 15th International Conference on E-Business Engineering (ICEBE)*, 78–85. https://doi.org/10.1109/ICEBE.2018.00022

Meis, R., & Heisel, M. (2017). Towards systematic privacy and operability (PRIOP) studies. *IFIP Advances in Information and Communication Technology*, *502*, 427–441. https://doi.org/10.1007/978-3-319-58469-0_29

Michael, J., Koschmider, A., Mannhardt, F., Baracaldo, N., & Rumpe, B. (2019). User-centered and privacy-driven process mining system design for IoT. *Lecture Notes in Business Information Processing*, *350*, 194–206. https://doi.org/10.1007/978-3-030-21297-1_17

Mohan, J., Wasserman, M., & Chidambaram, V. (2019). Analyzing GDPR Compliance Through the Lens of Privacy Policy. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11721 LNCS*, 82–95. https://doi.org/10.1007/978-3-030-33752-0_6

Morales-Trujillo, M. E., & Garcia-Mireles, G. A. (2018). Extending ISO/IEC 29110 Basic Profile with Privacy-by-Design Approach: A Case Study in the Health Care Sector. *2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC)*, 56–64. https://doi.org/10.1109/QUATIC.2018.00018

Morel, V., Cunche, M., & Métayer, D. L. (2019). A Generic Information and Consent Framework for the IoT. *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big*

Data Science And Engineering (TrustCom/BigDataSE), 366–373. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00056

Mougiakou, E., & Virvou, M. (2017). Based on GDPR privacy in UML: Case of e-learning program. *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 1–8.

Muller, D. A., & Lévy, P. (2019). A Design Approach towards Affording the Trend of Privacy. *Proceedings of the 2019 on Designing Interactive Systems Conference*, 435–446. https://doi.org/10.1145/3322276.3322324

Muntes-Mulero, V., Dominiaky, J., Gonzalezz, E., & Sanchez-Charles, D. (2019). Model-driven evidence-based privacy risk control in trustworthy smart IoT systems. *CEUR Workshop Proceedings*, *2442*, 23–30. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072775995&partnerID=40&md5=ae0378891ee2dfa9f5dee362352aa04d

Mustafa, U., Pflugel, E., & Philip, N. (2019). A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 1–9. https://doi.org/10.1109/ICGS3.2019.8688019

Neisse, R., Baldini, G., Steri, G., & Mahieu, V. (2016). Informed consent in Internet of Things: The case study of cooperative intelligent transport systems. *2016 23rd International Conference on Telecommunications (ICT)*, 1–5. https://doi.org/10.1109/ICT.2016.7500480

Notario, N., Ciceri, E., Crespo, A., Real, E. G., Catallo, I., & Vicini, S. (2017). Orchestrating Privacy Enhancing Technologies and Services with BPM Tools: The WITDOM Data

Protection Orchestrator. *Proceedings of the 12th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3098954.3104057

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376321

O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science*, *113*, 653–658. https://doi.org/10.1016/j.procs.2017.08.329

Olca, E., & Can, O. (2022). DICON: A Domain-Independent Consent Management for Personal Data Protection. *IEEE Access*, *10*, 95479–95497. https://doi.org/10.1109/ACCESS.2022.3204970

Palmirani, M., Rossi, A., Martoni, M., & Hagan, M. (2018). A methodological framework to design a machine-readable privacy icon set. *Jusletter IT*, *February*, Article February. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069718599&partnerID=40&md5=a5a320c360714b64b08b84845b3e34f4

Pandit, H. J., O'Sullivan, D., & Lewis, D. (2018). An ontology design pattern for describing personal data in privacy policies. *CEUR Workshop Proceedings*, *2195*, 29–39. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85053763584&partnerID=40&md5=5e3282d6de6cd147c191639ca82d4cea

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access*, *6*, 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522

Pardo, R., & Le Métayer, D. (2019). Analysis of privacy policies to enhance informed consent. *IFIP Annual Conference on Data and Applications Security and Privacy*, 177–198.

Pattakou, A., Mavroeidi, A.-G., Diamantopoulou, V., Kalloniatis, C., & Gritzalis, S. (2018). Towards the Design of Usable Privacy by Design Methodologies. *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, 1–8. https://doi.org/10.1109/ESPRE.2018.00007

Pedrosa, M., Costa, C., & Dorado, J. (2019). GDPR Impacts and Opportunities for Computer-Aided Diagnosis Guidelines and Legal Perspectives. *2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS)*, 616–621. https://doi.org/10.1109/CBMS.2019.00128

Pedroza, G., Muntés-Mulero, V., Martín, Y. S., & Mockly, G. (2021). A Model-based Approach to Realize Privacy and Data Protection by Design. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 332–339. https://doi.org/10.1109/EuroSPW54576.2021.00042

Perera, C., Barhamgi, M., & Vecchio, M. (2021). Envisioning Tool Support for Designing Privacy-Aware Internet of Thing Applications. *IEEE Internet of Things Magazine*, *4*(1), 78–83. https://doi.org/10.1109/IOTM.0001.2000006

Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J. B., Fiorani, M., Magkos, E., Sanz, A. C., Pavlidis, M., D'Addario, R., & Zorzino, G. G. (2019). DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11711 LNCS*, 78–93. https://doi.org/10.1007/978-3-030-27813-7_6

Rallo Lombarte, A. (2009, November 5). *International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution*. International Conference of Data Protection and Privacy Commissioners.

Regulation (EU) 2016/679. (2016). *On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.

Rhahla, M., Allegue, S., & Abdellatif, T. (2021). Guidelines for GDPR compliance in Big Data systems. *Journal of Information Security and Applications*, *61*. https://doi.org/10.1016/j.jisa.2021.102896

Roig, A. (2018). Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology*, *8*(3), Article 3.

Rossi, A., & Lenzini, G. (2020). Transparency by design in data-informed research: A collection of information design patterns. *Computer Law & Security Review*, *37*, 105402. https://doi.org/10.1016/j.clsr.2020.105402

Roubtsova, E., Roubtsov, S., & Alpár, G. (2018). Presence patterns and privacy analysis. *International Symposium on Business Modeling and Software Design*, 298–307.

Saatci, C., & Gunal, E. S. (2019). Preserving Privacy in Personal Data Processing. *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 1–4. https://doi.org/10.1109/UBMYK48245.2019.8965432

Schnädelbach, H., Jäger, N., & Urquhart, L. (2019). Adaptive Architecture and Personal Data. *ACM Trans. Comput.-Hum. Interact.*, *26*(2), Article 2. https://doi.org/10.1145/3301426

Shneiderman, B. (2000). Universal usability. *Communications of the ACM*, *43*(5), 84–91. https://doi.org/10.1145/332833.332843

Singh, J., & Cobbe, J. (2019). The Security Implications of Data Subject Rights. *IEEE Security Privacy*, *17*(6), Article 6. https://doi.org/10.1109/MSEC.2019.2914614

Sion, L., Dewitte, P., Landuyt, D. V., Wuyts, K., Emanuilov, I., Valcke, P., & Joosen, W. (2019). An Architectural View for Data Protection by Design. *2019 IEEE International Conference on Software Architecture (ICSA)*, 11–20. https://doi.org/10.1109/ICSA.2019.00010

Sion, L., Landuyt, D. V., Wuyts, K., & Joosen, W. (2019). Privacy Risk Assessment for Data Subject-Aware Threat Modeling. *2019 IEEE Security and Privacy Workshops (SPW)*, 64–71. https://doi.org/10.1109/SPW.2019.00023

Sion, L., Yskout, K., Van Landuyt, D., & Joosen, W. (2018). Solution-Aware Data Flow Diagrams for Security Threat Modeling. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1425–1432. https://doi.org/10.1145/3167132.3167285

Sobolewski, M., Mazur, J., & Paliński, M. (2017). GDPR: A step towards a user-centric internet? *Intereconomics*, *52*(4), Article 4. https://doi.org/10.1007/s10272-017-0676-5

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design—Dark patterns in cookie consent for online news outlets. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3419249.3420132

Sokolovska, A., & Kocarev, L. (2018). Integrating Technical and Legal Concepts of Privacy. *IEEE Access*, *6*, 26543–26557. https://doi.org/10.1109/ACCESS.2018.2836184

Spagnuelo, D., Bartolini, C., & Lenzini, G. (2017). Modelling metrics for transparency in medical systems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10442 LNCS*, 81–95. https://doi.org/10.1007/978-3-319-64483-7_6

Spagnuelo, D., Ferreira, A., & Lenzini, G. (2019). Accomplishing transparency within the general data protection regulation. *ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 114–125. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85064684301&partnerID=40&md5=10325896ebec8e07dfd643c343d74a5b

Stach, C., & Steimle, F. (2019). Recommender-Based Privacy Requirements Elicitation—EPICUREAN: An Approach to Simplify Privacy Settings in IoT Applications with Respect to the GDPR. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 1500–1507. https://doi.org/10.1145/3297280.3297432

Su, X., Hyysalo, J., Rautiainen, M., Riekki, J., Sauvola, J., Maarala, A. I., Hirvonsalo, H., Li, P., & Honko, H. (2016). Privacy as a service: Protecting the individual in healthcare data processing. *Computer*, *49*(11), Article 11.

Tahaei, M., Frik, A., & Vaniea, K. (2021). Privacy Champions in Software Teams: Understanding&nbsp;Their&nbsp;Motivations,&nbsp;Strategies,&nbsp;and&nbsp;Challenges. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445768

Tapsell, J., Akram, R. N., & Markantonakis, K. (2018). Consumer Centric Data Control, Tracking and Transparency – A Position Paper. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th*

IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1380–1385. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00191

Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Using Models to Enable Compliance Checking Against the GDPR: An Experience Report. *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*, 1–11. https://doi.org/10.1109/MODELS.2019.00-20

Ujcich, B. E., Bates, A., & Sanders, W. H. (2018). A provenance model for the european union general data protection regulation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11017 LNCS*, 45–57. https://doi.org/10.1007/978-3-319-98379-0_4

Urquhart, L. (2016). White Noise from the White Goods? Conceptual & Empirical Perspectives on Ambient Domestic Computing. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2865738

Urquhart, L., Sailaja, N., & Mcauley, D. (2018). Realising the Right to Data Portability for the Domestic Internet of Things. *Personal Ubiquitous Comput.*, *22*(2), Article 2. https://doi.org/10.1007/s00779-017-1069-2

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)Informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990. https://doi.org/10.1145/3319535.3354212

Veale, M., Binns, R., & Van Kleek, M. (2018). Some HCI priorities for GDPR-compliant machine learning. *Workshop at ACM CHI'18*. ACM CHI'18, Montreal, Canada.

Wachter, S. (2018a). *GDPR and the Internet of Things: Guidelines to Protect Users' Identity and Privacy*. SSRN.

Wachter, S. (2018b). Ethical and normative challenges of identification in the Internet of Things. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 1–10. https://doi.org/10.1049/cp.2018.0013

Wong, R. Y., & Mulligan, D. K. (2019). Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–17. https://doi.org/10.1145/3290605.3300492

Wright, S. A. (2019). Privacy in IoT Blockchains: With Big Data comes Big Responsibility. *2019 IEEE International Conference on Big Data (Big Data)*, 5282–5291. https://doi.org/10.1109/BigData47090.2019.9006341

Biographies

Marco Saltarella

Marco Saltarella graduated cum laude in computer engineering in 2018. In 2023 he received his PhD from the University of Bari with a research project on Usable Privacy. Since 2018 he is working in Fincons SpA where he is currently contributing to several European and Regional funded R&D projects.

Giuseppe Desolda

He is Assistant Professor at the Department of Computer Science, University of Bari, Italy. He is member of the Interaction Visualisation Usability (IVU) and UX Laboratory, where he coordinates research on novel interaction techniques, Internet of Things and usable security. He is a member of ACM, ACM SIGCHI, and SIGCHI Italy.

Rosa Lanzilotti

She is Associate Professor at the Computer Science Department, University of Bari, Italy. She is a member of the Interaction Visualization Usability (IVU) and UX Laboratory, where she coordinates research on usability engineering and UX. She is member of ACM, ACM SIGCHI, and SIGCHI Italy.

Vita Santa Barletta

She is an Assistant Professor at the Department of Computer Science, University of Bari, Italy. She is member of Software Engineering LABoratory (SERLAB) and her research interests include cybersecurity, quantum computing, quantum software engineering, secure software engineering, and secure project management.