Privacy Design Strategies and the GDPR: A Systematic Literature Review

Marco Saltarella[1,2], Giuseppe Desolda[1(✉)], and Rosa Lanzilotti[1]

[1] Department of Computer Science, University of Bari Aldo Moro, Bari, Italy
{marco.saltarella,giuseppe.desolda,rosa.lanzilotti}@uniba.it
[2] FINCONS SpA, Bari, Italy

Abstract. Article 25 of the GDPR states that data collection, processing and management measures should be implemented following tnhe privacy by design and privacy by default paradigms. This paper presents a systematic literature review to identify useful guidelines to support the development of GDPR-compliant software. Selected papers are categorized under 8 different data-oriented and process-oriented strategies and their contributions are reported. Future activities will highlight the HCI community's attitude towards these new technical and organizational approaches in order to bridge the identified gaps and shortcomings.

Keywords: GDPR · Privacy by design · Usable privacy

1 Introduction

In a world that is always online, with billions of connected devices, producing, exchanging and processing data, the cybersecurity risk has never been as threating. The University of Maryland estimated that a cyber-attack occurs every 39 s on average [90] representing a huge risk for our digital data-space. According to a report by IBM [91], the average cost of a data breach for a company is $3.86M with an average time to identify and contain the breach of 280 days. In this context, introducing effective security measures is fundamental not only to protect our digital assets but also to comply with the current normative.

In this regard, in May 2018 the European Union (EU) General Data Protection Regulation (GDPR) came into effectiveness, setting a new milestone in the data protection field, as the most advanced regulation related to the collection, management and processing of personal data. The GDPR demands that clear organizational and technical measures need to be implemented to guarantee specific principles and rights to data subjects. Specifically, as stated in Article 25, 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 to be as secure and privacy-preserving as possible) paradigms.

The term privacy by design was first defined by Ann Cavoukian whom in one of her most relevant studies defines the 7 foundational principles of privacy by design [92]: 1) Proactive not Reactive; Preventative not Remedial, 2) Privacy as the Default Setting, 3)

A. Moallem (Ed.): HCII 2021, LNCS 12788, pp. 241–257, 2021.
https://doi.org/10.1007/978-3-030-77392-2_16

Privacy Embedded into Design, 4) Fully Functionality – Positive-Sum, not Zero-Sum, 5) End-to-End Security – Full Lifecycle Protection, 6) Visibility and Transparency – Keep it Open, 7) Respect for User Privacy – Keep it User Centric.

These seven principles influenced and inspired the GDPR. If we focus the attention on the last principle, we can see how important is for Cavoukian that privacy is built around the user from the ground-up. Indeed, also the GDPR is seen as a step forward towards the user-centric approach [93]; however, due to the new technical challenges introduced by the regulation, the lack of usability for security and privacy features remains one of the most concerning issues. In the security field, the user has always been recognized as the weakest link of the chain [94]. Many studies have been carried out to understand how to address this problem on different levels [95, 96] and methodologies have been proposed [97]. Accordingly, it is necessary to consider advanced methodologies that support the design and development of GDPR compliant software to ensure the safeguarding of users' privacy while still maximizing the level of usability. By integrating the user-centric approach across all the development processes it is possible to implement innovative solutions that are secure and usable to satisfy, at the same time, both users' and businesses' objectives.

With the introduction of the GDPR, software engineers are now facing a new challenge: how to effectively translate the GDPR obligations into software requirements. Indeed, implementing these new requirements can be a daunting task [98], especially for developers that lack a baseline understating of both the legal and security concepts expressed in the regulation [99].

For these reasons, this paper presents a systematic literature review to frame the current best practices of GDPR-compliant software design and development implementing the privacy-by-design and privacy-by-default paradigms. After defining a rigorous research protocol in line with the guidelines proposed by Kitchenham et al. [101], more than 900 articles were collected from the major scientific digital libraries. Each article was assessed through specific inclusion and exclusion criteria in an iterative process to identify those that answer the defined research question. From the final selection of papers, the main results and lesson-learned were extracted and categorized under 8 different data-oriented and process-oriented, privacy design strategies [100]. The long-term goal of this work is to understand the impact that the new technical and organizational solutions implemented after the GDPR had on both users and developers, in order to address how to successfully satisfy both regulation constraints and users' privacy expectations. The knowledge acquired during this review will be useful to critically evaluate current solutions both from a security and a usability point of view and to identify what issues are still open to fill the gaps with future activities.

The paper is organized as follows: Sect. 2 describes the methodology followed for this systematic literature review. Section 3 presents and discusses the results of the review. Section 4 presents the conclusions and future work.

2 Methodology

To conduct this systematic literature review (SLR), a research protocol has been first defined following the guidelines proposed by Kitchenham et al. [101]. In line with this protocol, the following phases were carried out:

- *Planning*: including the definition of the research question, identification of relevant keywords and definition of the inclusion and exclusion criteria;
- *Execution*: retrieval of papers from the main research engines and iterative selection of the studies according to the defined inclusion and exclusion criteria;
- *Analysis*: extraction and discussion of relevant results to address the research questions.
- In the next sections, we report on the details of each phase.

2.1 Planning

Formulation of the Research Question
The first phase starts with the definition of the research question, which aim to address the main goal of this SLR, i.e., to systematize the current best practices of GDPR-compliant software design and development implementing privacy-by-design and privacy-by-default paradigms. In Article 25, the GDPR explicitly states that the data controller shall implement state-of-the-art technical and organizational measures to ensure data protection-by-design and default. Thus, the research question is:

RQ) *How to make effective the Privacy-By-Design and Privacy-By-Default paradigms during the design and development of GDPR compliant software?*

Definition of the Query String
In order to define the search string a set of keywords were identified: the main keywords (GDPR, privacy by design and privacy by default) were combined with related concepts (e.g., guidelines, patterns) in Boolean formula to discover relevant studies trying to answer the research question.

Thus, the following search query was defined:

```
(GDPR OR "General Data Protection Regulation") AND (pri-
vacy OR "privacy by design" OR "privacy by default" OR
security OR software) AND (engineering OR guidelines OR
"informed consent" OR patterns)
```

Selection of Data Sources
The query string was used to query 4 major digital libraries: ACM DL, IEEE Xplore, Scopus, Google Scholar.

Inclusion and Exclusion Criteria
To select articles that fit the research question, the following inclusion and exclusion criteria were defined:

Inclusion criteria:

- The article focuses on privacy-by-design and/or privacy-by-default for GDPR
- The article is published in a relevant journal or conference
- The article has been peer-reviewed

Exclusion criteria:

- The article is not focused on the GDPR
- The article is not related to ICT or HCI fields

2.2 Execution

The execution of the search string on all the scientific digital libraries resulted in 653 articles (ACM DL = 36, IEEE Xplore = 103, Scopus = 258, Google Scholar = 256). From these articles, 133 resulted duplicated and thus removed, obtaining a total of 520 paper to be analyzed. From this point on, an iterative selection process was conducted applying inclusion and exclusion criteria. First, articles were analyzed based on their title and abstract only. The application of the criteria allowed us to exclude 238 papers. After that, a more detailed analysis has been conducted by reading the whole manuscripts, leading to the selection of 91 papers.

3 Results Analysis

Data Extraction Strategy
The analysis of the 91 papers selected for the research question was based on "Privacy Design Strategies" [100], in which 8 different strategies are defined, with the aim of helping system designers translating in privacy-friendly way legal requirements into system requirements. These 8 strategies are divided in two sub-categories:

Category 1) Data-oriented strategies focused on the data processing itself:

1. Minimize: reduce the amount of data collected and processed to the minimum;
2. Separate: distribute data processing and storage;
3. Abstract: Limit the detail level of data processing as much as possible;
4. Hide: personal data should be hidden from unauthorized third-parties.

Category 2) Process-oriented strategies focused on the process handling the personal data lifecycle:

1. Inform: duly inform the users about the whole data processing lifecycle;
2. Control: empower the users with full control over their personal data;
3. Enforce: enforce a privacy-friendly data processing;
4. Demonstrate: demonstrate the enforcement of the privacy-friendly data processing.

Based on these eight categories, we extracted relevant results, best-practices, and guidelines from the selected papers. A table reporting the distribution of the papers inside each strategy, with a brief explanation of their contribution, is reported in Appendix ().

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

1. Minimize	
In order to avoid unnecessary disclosure, only data that is strictly needed should be displayed to users	4,9
Data to be processed should be carefully selected	9,70
Collection of data should be limited to only data required for the proper functionality of the application	14,40
Minimize data storage retention to reduce the risks associated with data breaches	40
2. Separate	
Adopt a MVC architecture	4
Process data in a distributed fashion through isolation and virtualization	9,29,70
Interconnect systems via overlay networks or message brokers	12,36
Separate users' data into sub-profile, in order to avoid account wide data breaches	12,44
Ensure cross-domain unlikability through context separation (physical and digital)	1,44
Opt for a Decentralized storage	40,84
3. Abstract	
Homomorphic encryption	5,40,37
k-anonymity	5,8,18,19,40,70,71
l-diversity	18,19,40
t-closeness	19,40
Derivation: replace detailed information with equivalent but more general ones (example: substitute Data of Birth with age)	18
Approximation: replace information with less specific one	18
Differential Privacy	5,8,19,70,71
Use Privacy aware data-analysis algorithms	8
Aggregate data over time	21,40,70
4. Hide	
Use Encryption both for storage and transfer	1,14,17,18,19,21,37,40,53,70,89
Use Anonymization at different layers and pseudonymization	1,3,4,11,15,16,19 ,20,21,28,37,44,52,63,69,70,78,89
Use Attribute Based Encryption and/or Attribute-Based Access Control	5,36,40,44,64

(*continued*)

Table 1. (*continued*)

Always use application layer protocols over TLS	5,11,14
Use Tor network	5,63,78
Never log sensitive information	17
Masking: delete or mask certain part of personal data (e.g.. Credit card number: 1234 **** **** 6789)	18
Mixing: if the only purpose of data is to derive descriptive statistics (mean, variance, etc.) the values can be mixed across the records to avoid detectability of individuals	18
Tokenization: replace data with a unique identifier that is used to retrieve the original value	18
5. Inform	
Privacy policy as a new ISO/IEC 29110 product. It should report how the data will be managed by the involved parties and regulate the process of requesting, storing, processing and disposing data	4
Explain the process of personal data processing in detailed, but concise and understandable way	9,24,42,48,53,73,75,84,88
Users must be explicitly informed about any data collection, sharing and processing taking place	14,21,22,23,48
Asking for a user's consent for processing his/her personal data must be separated from asking consent for other aspects of services offered by developers	9,14
Users must be informed about which data is collected for which duration and eventually how data from different sources is combined. Also the must be informed on how to request data removal and withdrawal of consent	21,23,42,48
At the level of policy, a list of third parties to which personal data may be forwarded should be maintained, together with the territories under the jurisdiction of which the third parties operate and associated legal justifications	48,23
Inform users about what data is necessary for the offered service and what data can be instead voluntarily shared	24
Cookie Consent is preferrable in the lower left corner (on desktop) or the bottom of the screen (on mobile)	31
Notify users of a policy update	42
Employ Transparency Enhancing Tools	27,58,60
Explain consequence of not providing data	48,73
Inform about data breach	48,72
Use Visual reminders	48,51,53,75,84

(*continued*)

Table 1. (*continued*)

6. Control	
Specify policies in a machine-readable format and automate the informed-consent process (e.g., by using P3P, PPL or LPL)	5,59,66,74,78,81
Users should be given a chance to learn and practice their rights (access, rectification, erasure, giving and withdrawing consent, and portability) through system UI	14,48,52,73,89
Service providers must enable users to withdraw their consent at any time	14,21,48,52,87,88,89
Service provider should offer the possibility to determine how long data can be stored for and who can access them	21
Consider client-side encryption	21
Consent should be provided in forms and at times that minimize users fatigue and maximize the likelihood that they make appropriate decisions	22,48,87
Provide options to access and update collected data and to opt-out from collection	48
Provide a Privacy dashboard to empower users full control on their data at any time	41,70
Move away from a take it or leave it and empower the user in choosing a balance between functionality and privacy	84,47
For IoT devices Disconnect options should be considered	88
7. Enforce	
Include privacy and data protection functions in general purpose engineering tools	2
Model driven design: Use Model Based Testing for verification of correct application of mechanisms for access control to personal data	2
Perform code Static Analysis	3,67
Define a Sensitive Data Dictionary to keep track of sensible data processed by the service	4
Use Role-Based Access Control / Functionality	4,16
Use Sticky policies	47,70,78,84
Use PkI or eIDAS supported Unique Identifier	12

(*continued*)

Table 1. (*continued*)

Personal data can be collected only if the current consent given by the data subject (external entity) covers the purpose of this collection Personal data can be collected only if this collection is logged At any moment, a data subject can request to change their current consent for what concerns the purpose of collection of their personal data	13,14
Recording, Usage, Disclosure and Retrieval of personal data can be performed only if mentioned in the current consent. Any of these operations must be logged. Personal data can be retained as recorded only if the current retention time given by the data subject has not expired. At any moment, a data subject can request to change their current consent	13,89
Enforce Strong password policy	14
By default, least privacy invasive choices should be selected for the users	16
Use models to support GDPR compliance and verification	25,33,34,35,43
During data portability requests: Users must be authenticated thought the service access control mechanism. Users must be notified of the event. Requested data should be available only for a limited time to avoid possible leakage	30,45
Awareness and education for the whole development team	39,48,65,76,90
Ontologies to model information related to personal data to improve interpretation, visualization and compliance checking against privacy policies	50,56,79,86
Execute a process to regularly assess test and evaluate the effectiveness of the technical and organizational measure concerned with the data processing	7,25,38,52,89
Constantly update anti-virus	53
Access by third parties is requested from user and agreed prior to disclosure	53
Support users' privacy expectation and ease the requirement elicitation process	54,83
Educate users	75,84
Employ HCI patterns to ease information access	77
Operationalize GDPR principles into relevant privacy requirements and use automated tests to continuously verify these requirements	85

(*continued*)

Table 1. (*continued*)

8. Demonstrate	
Performa a Data Protection Impact Assessment	1,6,10,16,23,24,32,88
Adopt a privacy threat modelling and management strategy (e.g. LINDDUN)	2,6,46,55,57,68,80,91
Log when sensitive information is being accessed and processed	3,4,9,11
Maintain database of cryptographically signed records of relevant information to "decide the accountability of any decision made"	12,23,26
Service Providers have to keep a record of users' consent decision and make it available on request	14,23,52,89
Data Controller to store the consents obtained from DS so they can demonstrate GDPR compliance	22,23
Enforce the Global Privacy Standard principles	61
Adopt a personal data-centric lifecycle model also to support the identification of critical activities and associated privacy risks	49,61,62,82

4 Discussion

As Table 1 in appendix shows, most of guidelines focus on process-oriented strategies. Specifically, solutions that propose models that help in complying with various GDPR directives are well discussed: in [2] the authors highlight how developers are not prepared to deal with privacy requirements and lack tools (and methods) to translate those requirements into the software. Thus, they suggest adopting a model-driven design to support engineers with GDPR compliant software development. In this sense, [56] proposes a data management model to make consent, specific and unambiguous enabling a GDPR compliant data processing (in line with the *enforce* strategy). Moreover, in [62] a UML-based data lifecycle model is proposed; in [33] the authors present a privacy-aware system design model to mitigate possible regulation violations during the design process; in [79] an ontology-based business process methodology to address GDPR requirements is presented.

The adoption of such methods also supports the *demonstrate* strategy enabling the compliance verification and transparency as directly requested by the GDPR. Among *demonstrate* guidelines, most authors seem to agree that performing a Data Protection Impact Assessment (DPIA), even in that cases that are not mandatory by the regulation, can help in complying with the GDPR as the DPIA is considered a powerful self-assessment tool. Along those lines, logging should be always performed when the user consents to processing and when accessing, processing, updating and deleting personal data [3]. To this end, indeed, users should always be given the opportunity to express their rights (*control* strategy). This, should also be implemented in a way that minimize fatigue while maximizing the likelihood for the user to make the appropriate decision

[22] and can be enabled, for example, by a privacy dashboard [70] or by supporting users' decision by using machine-readable policy formats [5, 78]. In any case, users should be able to always access and update collected data and to opt-out from collection [48]. Eventually, users could be provided the option to specify how long data can be stored and used for [21].

A relevant user-oriented solution worth mentioning is defined as "Sticky Policies", where users can define a set of rules that specifies how the data they are sharing shall be handled by service providers. However, this solution presents a few shortcomings that are addressed in [47].

On the other hand, service providers should move away from a take it or leave it approach [47] and leave users the choice of their preferred balance between functionality and privacy [84]. All of this should be provided in an agile fashion [88]. Nevertheless, service providers should distinguish between data necessary for using the service and data that can be, instead, voluntarily shared [24] (although as [14] and [40] suggest, only data exclusively required for the proper functionality of the service should be collected according to the *minimize* strategy) and consequences of not providing data should be explained [48, 73]. This falls under the *inform* strategy: users should always be explained the whole personal data process in a detailed but understandable and concise way [97]. Many authors agree that this could be supported by visual reminders [48]. To this end, [51] proposes a methodology to generate visual representations. However [88] argues that icons might not always be the best tool for communication.

Any policy update must be notified to users [42]. Users must be informed on what data is being collected and for what and for how long data will be stored [21]. However, the process of asking users consent must be separated from the choice of enabling other service-related features [9, 14].

Considering data-oriented strategies and specifically the *minimize* strategy, the amount of data collected and processed should be reduced to the minimum possible, and this should be decided on case by case basis [9, 70]. According to this strategy irrelevant information should be removed from the user's representation [4, 9]. Minimizing storage retention also reduces the risk associated with data breaches [40]. To this end, account wide data breaches can be avoided by adopting a *separate* strategy in which users' data is divided into sub-profiles [12, 44]. In any case, cross-domain unlinkability should be ensured by physical and digital separation [1, 44]. Decentralized storage [40, 84], isolation and virtualization [9, 70] and system interconnection via overlay networks or message brokers are also suggested [12, 36].

Many solutions are discussed under the *abstract* and *hide* strategies, including homomorphic encryption, k-anonymity, l-diversity, t-closeness and differential privacy. Data aggregation over time is also well suggested.

Anonymization and pseudonymization are the most common implementation of the *hide* strategy and encryption is always recommended both for storage and transfer. Attributed-Based Encryption is suggested as a method to easily provide both confidentiality and access control in a scalable way, without the need of a complex security infrastructure. Masking (hide part of the data), Mixing (mix data from multiple records) and Tokenization (replace data with unique ids) are also suggested as ways to implement this strategy [18].

In any case, it is worth to highlight how educating the development team [48] as well the end-users [84] is considered crucial to make these eight strategies effective. Indeed, education has always been a pillar of usable security and privacy [102]. However, educating, especially the end user, is a really ambitious and challenging task to achieve.

5 Conclusions and Future Work

This paper has presented a literature review that systematized current best-practices in designing and developing GDPR-compliant software following the by-design and by default paradigms. Selected studies were analyzed under different dimensions and categorized under Hoepman's design strategies. The analysis showed that from a technological point of view many different solutions exist to effectively support GDPR requirements implementation on different levels. However, there is still a lot to be done to make these tools and methods more user centered. 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 technical and methodological framework to support the user-centric design of GDPR-compliant software.

References

1. Mougiakou, E., Virvou, M.: Based on GDPR privacy in UML: case of e-learning program. In: 2017 8th International Conference on Information, Intelligence, Systems Applications (IISA), pp. 1–8 (2017). https://doi.org/10.1109/IISA.2017.8316456
2. Martin, Y., Kung, A.: Methods and tools for GDPR compliance through privacy and data protection engineering. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 108–111 (2018). https://doi.org/10.1109/EuroSPW.2018.00021
3. Hjerppe, K., Ruohonen, J., Leppänen, V.: The general data protection regulation: requirements, architectures, and constraints. In: 2019 IEEE 27th International Requirements Engineering Conference (RE), pp. 265–275 (2019). https://doi.org/10.1109/RE.2019.00036
4. Morales-Trujillo, M.E., Garcia-Mireles, G.A.: Extending ISO/IEC 29110 basic profile with privacy-by-design approach: a case study in the health care sector. In: 2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC), pp. 56–64 (2018). https://doi.org/10.1109/QUATIC.2018.00018
5. Li, C., Palanisamy, B.: Privacy in internet of things: from principles to technologies. IEEE Internet Things J. **6**, 488–505 (2019). https://doi.org/10.1109/JIOT.2018.2864168
6. Sion, L., et al.: An architectural view for data protection by design. In: 2019 IEEE International Conference on Software Architecture (ICSA), pp. 11–20 (2019). https://doi.org/10.1109/ICSA.2019.00010
7. Ayala-Rivera, V., Pasquale, L.: The grace period has ended: an approach to operationalize GDPR requirements. In: 2018 IEEE 26th International Requirements Engineering Conference (RE), pp. 136–146 (2018). https://doi.org/10.1109/RE.2018.00023
8. Sokolovska, A., Kocarev, L.: Integrating technical and legal concepts of privacy. IEEE Access. **6**, 26543–26557 (2018). https://doi.org/10.1109/ACCESS.2018.2836184
9. Colesky, M., Ghanavati, S.: Privacy shielding by design—a strategies case for near-compliance. In: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), pp. 271–275. IEEE (2016)

10. Coles, J., Faily, S., Ki-Aries, D.: Tool-supporting data protection impact assessments with CAIRIS. In: 2018 IEEE 5th International Workshop on Evolving Security Privacy Requirements Engineering (ESPRE), pp. 21–27 (2018). https://doi.org/10.1109/ESPRE.2018.00010
11. Badii, C., Bellini, P., Difino, A., Nesi, P.: Smart city IoT platform respecting GDPR privacy and security aspects. IEEE Access. **8**, 23601–23623 (2020). https://doi.org/10.1109/ACCESS.2020.2968741
12. Pedrosa, M., Costa, C., Dorado, J.: GDPR impacts and opportunities for computer-aided diagnosis guidelines and legal perspectives. In: 2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS), pp. 616–621 (2019)
13. Antignac, T., Scandariato, R., Schneider, G.: Privacy compliance via model transformations. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 120–126 (2018). https://doi.org/10.1109/EuroSPW.2018.00024
14. Hatamian, M.: Engineering privacy in smartphone apps: a technical guideline catalog for app developers. IEEE Access. **8**, 35429–35445 (2020). https://doi.org/10.1109/ACCESS.2020.2974911
15. Groen, E.C., Ochs, M.: CrowdRE, user Feedback and GDPR: towards tackling GDPR implications with adequate technical and organizational measures in an effort-minimal way. In: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), pp. 180–185 (2019). https://doi.org/10.1109/REW.2019.00038
16. Mustafa, U., Pflugel, E., Philip, N.: A novel privacy framework for secure M-Health applications: the case of the GDPR. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 1–9 (2019). https://doi.org/10.1109/ICGS3.2019.8688019
17. Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., Patsakis, C.: Security and privacy analysis of mobile health applications: the alarming state of practice. IEEE Access. **6**, 9390–9403 (2018). https://doi.org/10.1109/ACCESS.2018.2799522
18. Saatci, C., Gunal, E.S.: Preserving privacy in personal data processing. In: 2019 1st International Informatics and Software Engineering Conference (UBMYK), pp. 1–4 (2019). https://doi.org/10.1109/UBMYK48245.2019.8965432
19. Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M.: Privacy issues and data protection in big data: a case study analysis under GDPR. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 5027–5033 (2018). https://doi.org/10.1109/BigData.2018.8622621
20. Hiller, J., Schuldes, M., Eckstein, L.: Recognition and pseudonymization of data privacy relevant areas in videos for compliance with GDPR. In: 2019 IEEE Intelligent Transportation Systems Conference (ITSC), pp. 2387–2393 (2019). https://doi.org/10.1109/ITSC.2019.8917267
21. Mannhardt, F., Petersen, S.A., Oliveira, M.F.: Privacy challenges for process mining in human-centered industrial environments. In: 2018 14th International Conference on Intelligent Environments (IE), pp. 64–71 (2018). https://doi.org/10.1109/IE.2018.00017
22. Morel, V., Cunche, M., Métayer, D.L.: A generic information and consent framework for the IoT. In: 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), pp. 366–373 (2019)
23. Butin, D., Métayer, D.L.: A guide to end-to-end privacy accountability. In: 2015 IEEE/ACM 1st International Workshop on Technical and Legal aspects of data Privacy and Security, pp. 20–25 (2015). https://doi.org/10.1109/TELERISE.2015.12
24. Wachter, S.: Ethical and normative challenges of identification in the internet of things. In: Living in the Internet of Things: Cybersecurity of the IoT – 2018, pp. 1–10 (2018). https://doi.org/10.1049/cp.2018.0013

25. Torre, D., Soltana, G., Sabetzadeh, M., Briand, L.C., Auffinger, Y., Goes, P.: Using models to enable compliance checking against the GDPR: an experience report. In: 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS), pp. 1–11 (2019). https://doi.org/10.1109/MODELS.2019.00-20
26. Masmoudi, F., Sellami, M., Loulou, M., Kacem, A.H.: Optimal evidence collection for accountability in the cloud. In: 2018 IEEE 15th International Conference on e-Business Engineering (ICEBE), pp. 78–85 (2018). https://doi.org/10.1109/ICEBE.2018.00022
27. Tapsell, J., Akram, R.N., Markantonakis, K.: Consumer centric data control, tracking and transparency – a position paper. In: 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), pp. 1380–1385 (2018)
28. Damjanovic-Behrendt, V.: A Digital twin-based privacy enhancement mechanism for the automotive industry. In: 2018 International Conference on Intelligent Systems (IS), pp. 272–279 (2018). https://doi.org/10.1109/IS.2018.8710526
29. Ladjel, R., Anciaux, N., Pucheral, P., Scerri, G.: Trustworthy distributed computations on personal data using trusted execution environments. In: 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), pp. 381–388 (2019). https://doi.org/10.1109/TrustCom/BigDataSE.2019.00058
30. Singh, J., Cobbe, J.: The security implications of data subject rights. IEEE Secur. Priv. **17**, 21–30 (2019). https://doi.org/10.1109/MSEC.2019.2914614
31. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un) Informed consent: studying GDPR consent notices in the field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 973–990. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3319535.3354212
32. Ahmadian, A.S., Strüber, D., Riediger, V., Jürjens, J.: Supporting privacy impact assessment by model-based privacy analysis. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, pp. 1467–1474. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3167132.3167288
33. Ahmadian, A.S., Strüber, D., Jürjens, J.: Privacy-enhanced system design modeling based on privacy features. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 1492–1499. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3297280.3297431
34. Ahmadian, A.S., Jürjens, J., Strüber, D.: Extending model-based privacy analysis for the industrial data space by exploiting privacy level agreements. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, pp. 1142–1149. Association for Computing Machinery, New York (2018). https://doi.org/10.1145/3167132.3167256
35. Kupfersberger, V., Schaberreiter, T., Quirchmayr, G.: Security-driven information flow modelling for component integration in complex environments. In: Proceedings of the 10th International Conference on Advances in Information Technology. Association for Computing Machinery, New York (2018). https://doi.org/10.1145/3291280.3291797
36. Coroller, S., Chabridon, S., Laurent, M., Conan, D., Leneutre, J.: Position paper: towards end-to-end privacy for publish/subscribe architectures in the internet of things. In: Proceedings of the 5th Workshop on Middleware and Applications for the Internet of Things. pp. 35–40. Association for Computing Machinery, New York (2018). https://doi.org/10.1145/3286719.3286727
37. Notario, N., Ciceri, E., Crespo, A., Real, E.G., Catallo, I., Vicini, S.: Orchestrating privacy enhancing technologies and services with BPM tools: the WITDOM data protection orchestrator. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. Association for Computing Machinery, New York (2017). https://doi.org/10.1145/3098954.3104057

38. Diamantopoulou, V., Mouratidis, H.: Practical evaluation of a reference architecture for the management of privacy level agreements. Inf. Comput. Secur. **26**, 711–730 (2019). https://doi.org/10.1108/ICS-04-2019-0052
39. Lodge, T., Crabtree, A.: Privacy engineering for domestic IoT: enabling due diligence. Sensors (Switzerland) **19**, 4380 (2019). https://doi.org/10.3390/s19204380
40. Abdulghani, H.A., Nijdam, N.A., Collen, A., Konstantas, D.: A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective. Symmetry **11**, 774 (2019). https://doi.org/10.3390/sym11060774
41. Piras, L., et al.: DEFeND architecture: a privacy by design platform for GDPR compliance. In: Gritzalis, S., Weippl, E. R., Katsikas, S. K., Anderst-Kotsis, G., Tjoa, A. M., Khalil, I. (eds.) TrustBus 2019. LNCS, vol. 11711, pp. 78–93. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27813-7_6
42. Mohan, J., Wasserman, M., Chidambaram, V.: Analyzing GDPR compliance through the lens of privacy policy. In: Gadepally, V., et al. (eds.) DMAH/Poly -2019. LNCS, vol. 11721, pp. 82–95. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-33752-0_6
43. Agostinelli, S., Maggi, F. M., Marrella, A., Sapio, F.: Achieving GDPR compliance of BPMN process models. In: Cappiello, C., Ruiz, M. (eds.) Information Systems Engineering in Responsible Information Systems: CAiSE Forum 2019, Rome, Italy, June 3–7, 2019, Proceedings, pp. 10–22. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21297-1_2
44. Gabel, A., Schiering, I.: Privacy patterns for pseudonymity. IFIP Adv. Inf. Commun. Technol. **547**, 155–172 (2019). https://doi.org/10.1007/978-3-030-16744-8_11
45. Martino, M.D., Robyns, P., Weyts, W., Quax, P., Lamotte, W., Andries, K.: Personal information leakage by abusing the GDPR right of access. In: Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019, pp. 371–386 (2019)
46. Muntes-Mulero, V., Dominiaky, J., Gonzalezz, E., Sanchez-Charles, D.: Model-driven evidence-based privacy risk control in trustworthy smart IoT systems. In: CEUR Workshop Proceedings, pp. 23–30 (2019)
47. Gol Mohammadi, N., Leicht, J., Ulfat-Bunyadi, N., Heisel, M.: Privacy policy specification framework for addressing end-users' privacy requirements. In: Gritzalis, S., Weippl, E. R., Katsikas, S. K., Anderst-Kotsis, G., Tjoa, A. M., Khalil, I. (eds.) TrustBus 2019. LNCS, vol. 11711, pp. 46–62. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27813-7_4
48. Ataei, M., Degbelo, A., Kray, C., Santos, V.: Complying with privacy legislation: From legal text to implementation of privacy-aware location-based services. ISPRS Int. J. Geo-Inf. **7**, (2018). https://doi.org/10.3390/ijgi7110442
49. Ujcich, B., Bates, A., Sanders, W.: A Provenance model for the European union general data protection regulation. In: Belhajjame, K., Gehani, A., Alper, P. (eds.) IPAW 2018. LNCS, vol. 11017, pp. 45–57. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98379-0_4
50. Pandit, H.J., O'Sullivan, D., Lewis, D.: An ontology design pattern for describing personal data in privacy policies. In: CEUR Workshop Proceedings, pp. 29–39 (2018)
51. Palmirani, M., Rossi, A., Martoni, M., Hagan, M.: A methodological framework to design a machine-readable privacy icon set. In: Jusletter IT (2018)
52. Fernandes, M., Da Silva, A.R., Gonçalves, A.: specification of personal data protection requirements: analysis of legal requirements from the GDPR regulation. In: ICEIS 2018 - Proceedings of the 20th International Conference on Enterprise Information Systems, pp. 398–405 (2018)
53. O'Connor, Y., Rowan, W., Lynch, L., Heavin, C.: Privacy by design: informed consent and internet of things for smart health. In: Procedia Computer Science, pp. 653–658 (2017). https://doi.org/10.1016/j.procs.2017.08.329

54. Diamantopoulou, V., Angelopoulos, K., Pavlidis, M., Mouratidis, H.: A metamodel for GDPR-based privacy level agreements. In: CEUR Workshop Proceedings, pp. 299–305 (2017)
55. Martín, Y.-S., Del Álamo, J.M.: A meta model for privacy engineering methods. In: CEUR Workshop Proceedings, pp. 41–48 (2017)
56. Fatema, K., Hadziselimovic, E., Pandit, H., Debruyne, C., Lewis, D., O'Sullivan, D.: Compliance through informed consent: Semantic based consent permission and data management model. In: CEUR Workshop Proceedings (2017)
57. Meis, R., Heisel, M.: Towards systematic privacy and operability (PRIOP) studies. In: De Capitani di Vimercati, S., Martinelli, F. (eds.) SEC 2017. IAICT, vol. 502, pp. 427–441. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58469-0_29
58. Spagnuelo, D., Bartolini, C., Lenzini, G.: Modelling metrics for transparency in medical systems. In: Lopez, J., Fischer-Hübner, S., Lambrinoudakis, C. (eds.) TrustBus 2017. LNCS, vol. 10442, pp. 81–95. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-64483-7_6
59. Pardo, R., Le Métayer, D.: Analysis of privacy policies to enhance informed consent. In: Foley, S. (eds.) Data and Applications Security and Privacy XXXIII. DBSec 2019. Lecture Notes in Computer Science, vol. 11559, pp. 177–198, Springer, Cham https://doi.org/10.1007/978-3-030-22479-0_10
60. Spagnuelo, D., Ferreira, A., Lenzini, G.: Accomplishing transparency within the general data protection regulation. In: 5th International Conference on Information Systems Security and Privacy. To appear (2018)
61. Alshammari, M., Simpson, A.: Towards a principled approach for engineering privacy by design. In: Schweighofer, E., Leitold, H., Mitrakas, A., Rannenberg, K. (eds.) Privacy Technologies and Policy, APF 2017. Lecture Notes in Computer Science, vol. 10518, pp. 161–177. Springer, Cham https://doi.org/10.1007/978-3-319-67280-9_9
62. Alshammari, M., Simpson, A.: A UML profile for privacy-aware data lifecycle models. In: Katsikas, S. et al. (eds.) Computer Security, SECPRE 2017, CyberICPS 2017, Lecture Notes in Computer Science, vol. 10683, pp. 189–209 Springer, Cham. https://doi.org/10.1007/978-3-319-72817-9_13
63. Diamantopoulou, V., Argyropoulos, N., Kalloniatis, C., Gritzalis, S.: Supporting the design of privacy-aware business processes via privacy process patterns. In: 2017 11th International Conference on Research Challenges in Information Science (RCIS), pp. 187–198. IEEE (2017)
64. Michael, J., Koschmider, A., Mannhardt, F., Baracaldo, N., Rumpe, B.: User-centered and privacy-driven process mining system design for IoT. In: Cappiello, C., Ruiz, M. (eds.) Information Systems Engineering in Responsible Information Systems: CAiSE Forum 2019, Rome, Italy, June 3–7, 2019, Proceedings, pp. 194–206. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21297-1_17
65. Hadar, I., et al.: Privacy by designers: software developers' privacy mindset. Empirical Softw. Eng. **23**(1), 259–289 (2017). https://doi.org/10.1007/s10664-017-9517-1
66. Gerl, A., Bennani, N., Kosch, H., Brunie, L.: LPL, towards a GDPR-compliant privacy language: formal definition and usage. In: Hameurlain, A., Wagner, R. (eds.) Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVII, pp. 41–80. Springer, Berlin (2018). https://doi.org/10.1007/978-3-662-57932-9_2
67. Ferrara, P., Spoto, F.: Static analysis for GDPR compliance. In: ITASEC (2018)
68. Sion, L., Van Landuyt, D., Wuyts, K., Joosen, W.: Privacy risk assessment for data subject-aware threat modeling. In: 2019 IEEE Security and Privacy Workshops (SPW), pp. 64–71. IEEE (2019)
69. Hillen, C.: The pseudonym broker privacy pattern in medical data collection. In: 2015 IEEE Trustcom/BigDataSE/ISPA, pp. 999–1005. IEEE (2015)

70. Kung, A., et al.: A privacy engineering framework for the internet of things. In: Kung, A., et al.: A privacy engineering framework for the internet of things. In: Data Protection and Privacy: (In) visibilities and Infrastructures, pp. 163–202. Springer, Cham (2017)
71. Roig, A.: Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). Eur. J. Law Technol. **8**, (2018)
72. Roubtsova, E., Roubtsov, S., Alpár, G.: Presence patterns and privacy analysis. In: Shishkov, B. (ed) Business Modeling and Software Design, BMSD 2018, Lecture Notes in Business Information Processing, vol. 319, pp. 298–307. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94214-8_21
73. Betzing, J.H., Tietz, M., vom Brocke, J., Becker, J.: The impact of transparency on mobile privacy decision making. Electron. Markets 1–19 (2019)
74. Su, X., et al.: Privacy as a service: protecting the individual in healthcare data processing. Computer **49**, 49–59 (2016)
75. G Karácsony, G.: Managing Personal Data in a Digital Environment-Did GDPR's Concept of Informed Consent Really Give Us Control? In: International Conference on Computer Law, AI, Data Protection & The Biggest Tech Trends. (2019).
76. Li, Z.S., Werner, C., Ernst, N., Damian, D.: GDPR Compliance in the Context of Continuous Integration. arXiv preprint arXiv:2002.06830. (2020)
77. Loruenser, T., Pöhls, H.C., Sell, L., Laenger, T.: CryptSDLC: Embedding cryptographic engineering into secure software development lifecycle. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, pp. 1–9 (2018)
78. Martucci, L. A., Fischer-Hübner, S., Hartswood, M., Jirotka, M.: Privacy and social values in smart cities. In: Angelakis, Vangelis, Tragos, Elias, Pöhls, Henrich C., Kapovits, Adam, Bassi, Alessandro (eds.) Designing, Developing, and Facilitating Smart Cities, pp. 89–107. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-44924-1_6
79. Bartolini, C., Muthuri, R., Santos, C.: Using ontologies to model data protection requirements in workflows. In: Otake, M., Kurahashi, S., Ota, Y., Satoh, K., Bekki, D. (eds.) New Frontiers in Artificial Intelligence, pp. 233–248. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-50953-2_17
80. Sion, L., Yskout, K., Van Landuyt, D., Joosen, W.: Solution-aware data flow diagrams for security threat modeling. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. pp. 1425–1432 (2018)
81. Neisse, R., Baldini, G., Steri, G., Mahieu, V.: Informed consent in internet of things: the case study of cooperative intelligent transport systems. In: 2016 23rd International Conference on Telecommunications (ICT). pp. 1–5. IEEE (2016)
82. Alshammari, M., Simpson, A.: Personal Data Management for Privacy Engineering: An Abstract Personal Data Lifecycle Model. Oxford, UK, CS-RR-17–02 (2017)
83. Stach, C., Steimle, F.: Recommender-based privacy requirements elicitation-EPICUREAN: an approach to simplify privacy settings in IoT applications with respect to the GDPR. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 1500–1507 (2019)
84. Custers, B., Dechesne, F., Pieters, W., Schermer, B.W., van der Hof, S.: Consent and privacy. In: Müller A., Schaber, P. (eds.) The Routledge Handbook of the Ethics of Consent. Routledge, London, pp. 247–258 (2018)
85. Agarwal, S., Steyskal, S., Antunovic, F., Kirrane, S.: Legislative compliance assessment: framework, model and GDPR instantiation. In: Medina, M., Mitrakas, A., Rannenberg, K., Schweighofer, E., Tsouroulas, N. (eds.) Privacy Technologies and Policy, APF 2018, Lecture Notes in Computer Science, vol. 11079, pp. 131–149. Springer, Cham (2018)
86. Besik, S., Freytag, J.-C.: A formal approach to build privacy-awareness into clinical workflows. SICS Softw-Intensive Cyber-Phys. Syst. **35**(1–2), 141–152 (2019). https://doi.org/10.1007/s00450-019-00418-5

87. Hyysalo, J., Hirvonsalo, H., Sauvola, J., Tuoriniemi, S.: Consent management architecture for secure data transactions. In: ICSOFT 2016 - Proceedings of the 11th International Joint Conference on Software Technologies, pp. 125–132 (2016). https://doi.org/10.5220/0005941301250132
88. Wachter, S.: GDPR and the Internet of Things: Guidelines to Protect Users' Identity and Privacy. SSRN (2018)
89. Al-Momani, A., Kargl, F., Schmidt, R., Kung, A., Bösch, C.: A privacy-aware v-model for software development. In: 2019 IEEE Security and Privacy Workshops (SPW), pp. 100–104 (2019). https://doi.org/10.1109/SPW.2019.00028
90. University of Maryland Study: Hackers Attack Every 39 Seconds. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. Accessed 02 Nov 2021
91. IBM Security Cost of a Data Breach Report 2020 https://www.ibm.com/security/data-breach. Accessed 02 Nov 2021
92. Cavoukian, A.: Privacy by design: The 7 foundational principles. Inf. Priv. Commissioner **5**, 12 (2009)
93. Sobolewski, M., Mazur, J., Paliński, M.: Gdpr: a step towards a user-centric internet? Intereconomics **52**(4), 207–213 (2017)
94. Leach, J.: Improving user security behaviour. Comput. Secur. **22**(8), 685–692 (2003)
95. Schultz, E.E., Proctor, R.W., Lien, M.C., Salvendy, G.: Usability and security an appraisal of usability issues in information security methods. Comput. Secur. **20**(7), 620–634 (2001)
96. Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., Cranor, L.F.: Crying wolf: an empirical study of SSL warning effectiveness. In: USENIX security symposium (SSYM 2009), pp. 399–416 (2009)
97. Muñoz-Arteaga, J., González, R.M., Martin, M.V., Vanderdonckt, J., Álvarez-Rodríguez, F.: A methodology for designing information security feedback based on user interface patterns. Adv. Eng. Softw. **40**(12), 1231–1241 (2009)
98. Urquhart, L., Rodden, T: A Legal Turn in Human Computer Interaction? Towards "Regulation by Design" for the Internet of Things. Available at SSRN: https://ssrn.com/abstract=2746467 (2016)
99. Martin, Y.S., Kung, A.: Methods and tools for GDPR compliance through privacy and data protection engineering. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 108–111 (2018)
100. Hoepman, J.-H.: Privacy design strategies. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds.) SEC 2014. IAICT, vol. 428, pp. 446–459. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55415-5_38
101. Kitchenham, B.: Procedures for performing systematic reviews. Keele UK Keele Univ. **33**, 1–26 (2004)
102. Sasse, M.A., Flechais, I.: Usable security: why do we need it? how do we get it? In: Cranor, L.F., Garfinkel, S. (eds.) Security and Usability: Designing secure systems that people can use, pp. 13–30. O'Reilly, Sebastopol (2005)