Privacy impact assessments in the wild: A scoping review

(article starts on next page)

Privacy impact assessments in the wild: A scoping review

Leonardo Horn Iwaya [a,*], Ala Sarah Alaqra [b], Marit Hansen [c], Simone Fischer-Hübner [a,d]

[a] Department of Mathematics and Computer Science, Karlstad University, Universitetsgatan 2, Karlstad, 651 88, Värmland, Sweden
[b] Information Systems, Karlstad Business School, Karlstad University, Universitetsgatan 2, Karlstad, 651 88, Värmland, Sweden
[c] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstraße 98, Kiel, 24103, Schleswig-Holstein, Germany
[d] Department of Computer Science and Engineering Chalmers University of Technology, Rännvägen 6B, Gothenburg, 412 96, Västra Götaland, Sweden

ARTICLE INFO

ABSTRACT

Privacy Impact Assessments (PIAs) offer a process for assessing the privacy impacts of a project or system. As a privacy engineering strategy, they are one of the main approaches to privacy by design, supporting the early identification of threats and controls. However, there is still a shortage of empirical evidence on their use and proven effectiveness in practice. To better understand the current literature and research, this paper provides a comprehensive Scoping Review (ScR) on the topic of PIAs "in the wild," following the well-established Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) guidelines. This ScR includes 45 studies, providing an extensive synthesis of the existing body of knowledge, classifying types of research and publications, appraising the methodological quality of primary research, and summarising the positive and negative aspects of PIAs in practice, as reported by those studies. This ScR also identifies significant research gaps (e.g., evidence gaps from contradictory results and methodological gaps from research design deficiencies), future research pathways, and implications for researchers, practitioners, and policymakers developing and using PIA frameworks. As we conclude, there is still a significant need for more primary research on the topic, both qualitative and quantitative. A critical appraisal of qualitative studies revealed deficiencies in the methodological quality, and only four quantitative studies were identified, suggesting that current primary research remains incipient. Nonetheless, PIAs can be regarded as a prominent sub-area in the broader field of empirical privacy engineering, in which further scientific research to support existing practices is needed.

Contents

* Corresponding author.
  E-mail address: leonardo.iwaya@kau.se (L.H. Iwaya).

1. Introduction

A Privacy Impact Assessment (PIA) has been defined by Wright [1] as a *"methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts"*. It is a process that should begin at the earliest possible stage of a project and should continue even after the project has been implemented [1]. PIAs emerged in the last century as a specific form of Technology Assessment and have become progressively more commonly used in practice from the mid-1990s onwards [2].

A related methodology is a Data Protection Impact Assessment (DPIA), which has been incorporated into the EU General Data Protection Regulation (GDPR) [3]. Article 35 of the GDPR requires that for technologies that are *"likely to result in a high risk to the rights and freedoms of natural persons",* the controller shall conduct an assessment of the impact of the envisaged processing operations on the protection of personal data. Article 36 additionally requires "prior consultation" with the data protection supervisory authority for any data processing project for which a DPIA indicates a high risk with no identified set of measures to sufficiently mitigate the risk.

Hence, with the GDPR that came into force in 2016, a DPIA is now defined more formally, and data controllers are required to make an assessment of the impact on data protection, which means specifically in relation to the GDPR data protection principles stated in Article 5. Formally, the right to data protection can be derived from Article 8 of the Charter of Fundamental Rights of the European Union (CFR) [4], whereas privacy is addressed in Article 7 of the CFR. However, the differentiation between privacy and data protection may be regarded as not as important for DPIA and PIA since, in the European sense, PIA has never been strictly separated from data protection. Moreover, Article 35 of the GDPR requires an assessment of technologies posing a high risk to the rights and freedoms of natural persons, which includes other fundamental rights (beyond the right to data protection) [5], including the right to privacy pursuant to Article 7 of the CFR. Consequently, in the remainder of this paper, we do not strictly distinguish between PIAs and DPIAs, meaning that the investigation of PIAs in this paper will also address DPIAs.

The overall objective of this paper is to provide a Scoping Review (ScR) to analyse the state of PIAs in practice ("in the wild") addressed by the research community and documented by the scientific literature. By PIA in practice, we mean empirical experience, application, and practical use of PIAs in real-world settings. We are particularly interested in elaborating on the positive aspects of PIAs (enablers, opportunities, drivers, and advantages) and the negative aspects (barriers, challenges, hindrances, and disadvantages), as reported by the scientific literature.

Although prior work on PIAs sometimes regards them as commonplace [6] and widespread [7,8], other studies have found that they are not commonly known and used by practitioners [9,10]. Additionally, empirical studies have also pointed to a low prevalence of PIAs for highly sensitive systems, such as mobile health apps [11]. Such problems have motivated this study to survey the research field of PIAs in practice systematically, including the positive and negative aspects of PIAs that are experienced, and to gain more knowledge in order to understand the state of the art.

An earlier related investigation by Wright [1] on the state of the art of PIAs and their advantages, based on findings from the Privacy Impact Assessment Framework (PIAF) project, was (in contrast to our work) not published as a systematic review based on a well-defined protocol. It also dates back to 2012, before the GDPR was in force, and can thus not be regarded as up to date. Another descriptive field study on PIAs in practice is based on interviews with data protection officers and restricted to organisations in the Netherlands [12]. To the best of our knowledge, no related work on this topic has been published yet in the form of a systematic literature or scoping review that also considers recent research literature.

This ScR is based on 45 publications chosen following a formal review protocol and procedure. As we show below in Section 4.1, more than half of the studies on this topic (included in this review) were only published after 2016. However, publications before 2016 (before the year when the GDPR came into force) have rarely considered the DPIA context that the GDPR now gives. They were rather based on PIAs following their own ideas on what to assess, which were not necessarily the data protection principles of the GDPR, and not necessarily – which is even more important – risks related to the rights and freedoms of natural persons.

As a result, the contributions of this article are threefold: (i) a comprehensive synthesis of PIAs in practice, summarising existing research, main methodologies, and positive and negative aspects; (ii) a quality appraisal of existing qualitative and quantitative research on the topic; and (iii) a detailed discussion of identified research gaps and possible pathways for future research. These contributions benefit many stakeholders (e.g., privacy researchers, practitioners, law and policymakers) involved in the development and performance of PIAs. Privacy researchers can better understand the state of the art and pathways for future work on the practical aspects of PIAs. Practitioners responsible for carrying out PIAs in practice can further understand the barriers and enablers of the PIA process, select better approaches based on more knowledge and avoid pitfalls. Law and policymakers can also use the evidence-based insights of this review when developing guidelines, policies, and regulations, as well as when consulting with organisations.

The remainder of this article is structured as follows: Section 2 presents the background information and prior work; Section 3 provides the details of the ScR methodology that guided this research; Section 4 presents the research results, including an account of the nature of existing evidence, a summary of the positive and negative aspects of PIAs in practice, and a critical appraisal of identified primary research; Section 6 describes the limitations of this ScR; Section 5 discusses the main findings and implications; and Section 7 concludes the paper.

2. Background

2.1. PIAs are more than DPIAs

The terms PIA and DPIA are often used interchangeably, but it is important to clarify that they differ. As briefly mentioned in the introduction, the concept of PIA far predates the EU framework GDPR and its legal requirement for DPIAs. PIAs come from a longer history, particularly in English-speaking countries, concerned with assessing the impact of technologies on people's privacy rights – for a historical review of the origins of PIAs, we refer readers to the work of Clarke [2]. Nonetheless, GDPR has indeed motivated a great deal of research on PIA methodologies that assist practitioners in their attempts to systematise this process. Such methodologies are, however, explicitly named as "PIAs", that is, adhering to the multi-dimensional concept of "privacy" rather than the narrower concept of "data protection", as defined in the GDPR and Article 8 of the CFR. Some of the widely known PIA methodologies include:

- New Zealander PIA Handbook [13];

- German PIA guidelines [14,15];
- French PIA Methodology [16];
- Australian PIA Guide [17]; and,
- ISO/IEC 29134 Guidelines for PIAs [18].

On the other hand, the DPIA is an instrument introduced by Article 35 of the GDPR [3]. Notice that the terminology starting with "data protection" was chosen consistently with the name of the law itself, that is, General "Data Protection" Regulation. However, well before the GDPR, policymakers and academics had already established the notion of PIAs. To some extent, DPIA becomes a new label for something already existing. In fact, when the Article 29 Working Party, the former body encompassing the data protection supervisory authorities from the European Union and predecessor of the European Data Protection Board, later created guidelines and recommendations on the conduction of "DPIAs", they actually pointed to a series of well-known PIA methodologies (see Annex 1 of WP29 [19]). In this paper, given this context, we use the term PIAs more often, referring to a methodology that is common to many other countries and jurisdictions. The term DPIA is used to refer to PIAs as a legal requirement specific to Europe, based on the GDPR. Thus, DPIAs can be considered as a part of the broader area of PIA methodologies.

2.2. Approaches to PIAs

It is also important to clarify that PIA methodologies come in all shapes and sizes. For instance, some general methodologies were proposed by data protection authorities in different countries, such as previously mentioned ones in New Zealand [13], Germany [14], and France [16]. Some methodologies can be considered industry- or application-specific, such as the PIA for RFID systems [15], the PIA for Smart Grids [20], or the PIA template for provenance systems [21].

PIA methodologies can be differentiated regarding their comprehensiveness and depth of the assessment, sometimes deemed as *lightweight* or *full-fledged*. For instance, the PIA template for mobile health applications proposed by Mantovani et al. [22] consists of a concise questionnaire, which can be considered lightweight. The work of Schneider et al. [23] also proposed a software-based instrument that could serve as the low-threshold entry point for non-experts to start with DPIAs. However, while smaller businesses may be tempted to rely on such lightweight approaches, it should be noted that data protection supervisory authorities may not be satisfied with the result of such assessments. Therefore, full-fledged methodologies are more often recommended, which include many of the methodologies developed by privacy agencies (e.g., [13,16,17,24]) and risk-based methodologies (e.g., [14–16, 18,25]) that borrow from traditional risk assessment theories, using the notions of threats and risks (i.e., with severity and likelihood levels).

This manuscript does not intend to review existing PIA methodologies comprehensively. Therefore, we refer the readers to important contributions in the area in which the authors have already theoretically compared and evaluated the most common PIA methodologies, as in the works of Vemou and Karyda [26,27] and Bisztray and Gruschka [28]. Furthermore, a systematic review of the scientific evidence on the *evaluation* and *validation* of PIA methodologies has also been presented by Wairimu et al. [29]. It is worth stressing, however, that the work of Wairimu et al. [29] dealt exclusively with *scientific* PIA methodologies, which are seldom employed in practice, as also evidenced by the results of this ScR.

3. Methods

This study follows Scoping Review (ScR) protocols according to the Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) [30], and adheres to the PRISMA-P [31] checklist for the research protocol to ensure the completeness and transparency of the review process. An ScR is a type

of systematic review used to map key concepts underpinning a research area and the main sources and types of evidence available [32]. This type of review emphasises a comprehensive coverage (i.e., breadth) of available literature [32] and is used to identify knowledge gaps, set research agendas, and identify implications for decision-making [33]. For this reason, it is worth mentioning that ScRs can also be considered as a preliminary type of systematic review that can later be narrowed down to more targeted topics for systematic literature reviews (SLRs) [34]. The main phases and steps of this ScR are presented as follows.

3.1. Phase I — Planning the ScR

3.1.1. Research questions

This study started with the objective of understanding the literature and research on the topic of PIAs in practice. Here, we are focusing on empirical evidence that deals with the experience, application, and practical use of PIAs in real-world settings. To meet this overarching objective, three guiding Research Questions (RQs) were formulated:

- **RQ1:** *What literature and research discuss and/or evaluate the use of PIAs in practice?* **Objective:** To identify the existing research and understand the types of studies and contributions in the literature, as well as the methodological approaches used, main venues, industry sectors, laws and regulations.
- **RQ2:** *What are the main methodologies and positive and negative aspects of PIAs in practice as reported in the literature?* **Objective:** To identify relevant characteristics, such as the main methodologies reported in the studies, and compile shared experiences, focusing on understanding the main positive and negative aspects related to PIAs in practice.
- **RQ3:** *What is the state of existing primary research studies on the topic?* **Objective:** To further examine and critically appraise existing primary research and to identify the studies (or the lack thereof) that have proposed valid and reliable instruments related to PIAs.

3.1.2. Identifying the need for the review

Before undertaking the ScR, it is important to verify whether reviews have already been published on the topic. To do so, five scientific databases (Google Scholar, Scopus, IEEE Xplore, ACM Digital Library, and Web of Science) were searched using the keywords: *"review"*, *"survey"*, *"privacy impact assessment*"*, and *"data protection impact assessment*"*. No surveys or systematic reviews were found, confirming the need for this ScR and revealing a lack of secondary research on PIAs.

3.1.3. Writing the ScR protocol

In preparation for the review, a ScR research protocol is written detailing all the systematic steps to be followed. This protocol was then discussed among the researchers and piloted, allowing us to refine search strategies and achieve a common understanding. The final protocol for this ScR is provided in [35] together with a replication package [36]. Therefore, we refer the readers to these documents for extensive methodological details and supplementary materials.

3.2. Phase II — Conducting the ScR

3.2.1. Information sources and search process

Due to their size and relevance to computer science and engineering, four databases were searched, including Scopus, Web of Science, IEEE Xplore, and ACM Digital Library. The searches were done on 01/Nov/2023 without setting restrictions (e.g., year limits, publication types, etc.). A structured search strategy was performed based on the RQs using the following general search string: `"privacy impact assessment*" OR "data protection impact assessment*"`. Later, when reading the selected papers, backward and forward snowballing searches were also performed. Although grey literature was also searched using the OpenGrey Database (www.opengrey.eu), no relevant studies were found.

3.2.2. Eligibility criteria

To meet the eligibility criteria, publications must address both aspects: (1) PIAs or DPIAs; and their (2) practice, application, and empirical experience. Studies that discuss or more profoundly evaluate the use of PIAs in practice through the lens of many stakeholders (e.g., privacy officers, policymakers, data subjects, etc.) were also considered. However, the exclusion criteria refer to studies that only present a purely theoretical contribution, without any practical component (e.g., a study in a real-world setting or with real practitioners/stakeholders), such as studies that propose, compare, or validate PIAs solely on a hypothetical basis or "illustrative" use case scenarios. Furthermore, it is worth noting that Scoping Reviews should include all types of studies (e.g., opinion papers, experience papers, primary studies, evaluation studies), emphasising the breadth of literature and not being limited to exclusively primary research papers.

3.2.3. Selection of studies

The results from each database were then exported separately (i.e., RIS files) and imported into the Rayyan software (www.rayyan.ai), a collaborative web tool that supports the screening process in systematic reviews. Rayyan automatically generates a list of duplicate entries, which the reviewers can easily check and manually remove. Two reviewers in double-blind mode performed this screening process using Rayyan. Before going through all the retrieved studies, the reviewers performed a calibration round to ensure a common understanding and minimise uncertainties about the eligibility criteria (see Section 3.2.2). The selection of studies follows two main steps: Step (1) reading of titles and abstracts; and, Step (2) full reading of the studies. In Step 1, two reviewers used separate Rayyan accounts to analyse the whole list of retrieved studies. Based on the eligibility criteria, the reviewers decided whether to "exclude" or "include" the study for further analysis in Step 2. In case of disagreements, a third reviewer was called to establish the final decision. In Step 2, the full-texts of all studies included so far were downloaded and screened by the two reviewers again, following the eligibility criteria. If any reviewer deemed a study to be outside the scope, the study was discussed with a third reviewer for a final decision.

3.2.4. Data extraction and data charting processes

A data extraction form was created, tested, and discussed among the research team – available in [36]. This form facilitates the consistent extraction of relevant data from each publication in separate files. This data extraction step later facilitated the data charting process. Data extraction was an iterative process, allowing reviewers to critique, agree, and update the data extraction form as needed. Only direct quotes were extracted from the studies to ensure accuracy. Established classification schemes were used to classify (a) Types of Research and (b) Types of Contributions. The categories proposed by Wieringa et al. [37] and Creswell and Creswell [38] were used for the research types. Furthermore, the classification proposed by Shaw [39] is used for contribution types. Nonetheless, notes were always included in the form to justify any classification choices.

3.3. Phase III — Reporting the ScR

3.3.1. Synthesis of results

The synthesis of results aims to combine data from included studies into a coherent narrative using tables, charts, and classifications. This is facilitated by the data charting performed parallel to the data extraction steps. Two groups of data were generated: quantitative data (e.g., year of publication, publications per author, citations) and qualitative data (e.g., type of publication, type of research, type of contribution). Reviewers could then perform the synthesis via spreadsheet and text software (LibreOffice Calc and Writer), generating tables and figures, interpreting findings, and providing a descriptive mapping of the body
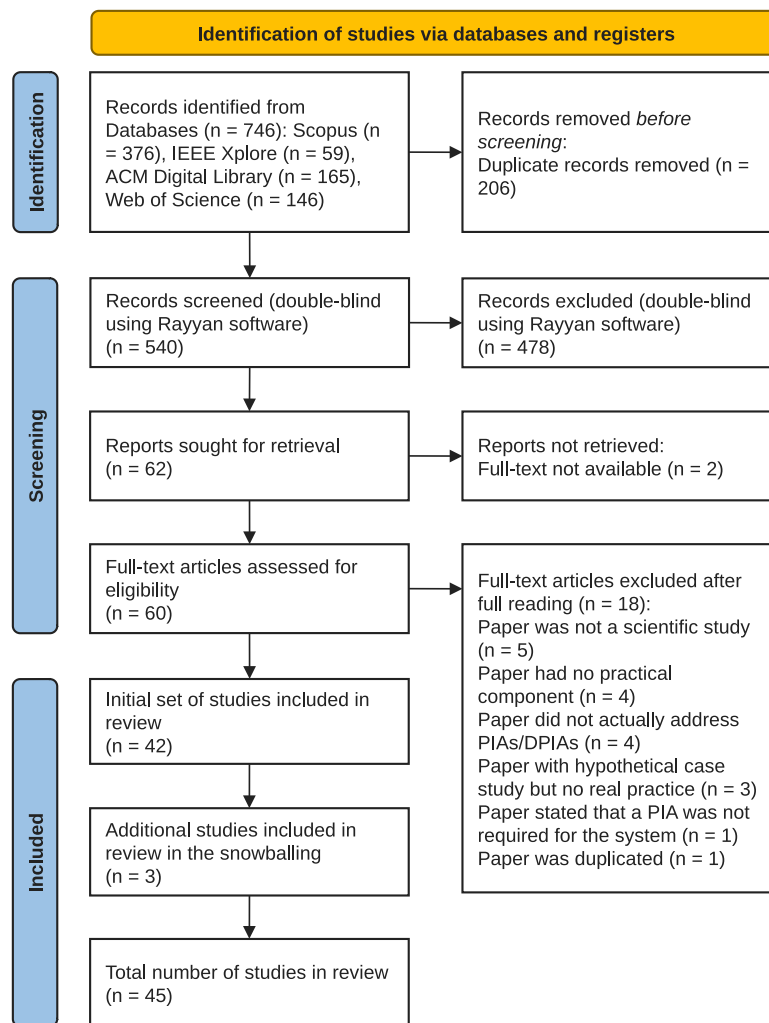
Fig. 1. PRISMA flowchart for this ScR.

of knowledge. Thus, a coherent narrative was written to convey all results, interpret the main findings, and discuss research gaps.

As part of the narrative summary, we derived from the literature a series of positive and negative aspects of PIAs in practice to answer RQ2. To do so, excerpts and quotes from the studies that reflected on such positive and negative aspects were captured in the data extraction step and later analysed by the researchers. A thematic analysis methodology [40] was employed to code all the extracted materials qualitatively – the NVivo software was used. This process was led by one researcher, initiating it with open coding under two broad themes (i.e., (1) positive and (2) negative aspects). With the help of two other researchers, all the generated codes were then revised for a shared understanding of their names, descriptions, and consistency with the original excerpts and quotes. The codes were then organised into sub-themes. The group of three researchers iterated continuously through the list of sub-themes and codes until a consensus was reached on the resulting sub-themes.

3.3.2. Critical appraisal of primary research

During the synthesis, it was found that a critical appraisal of primary research was justified. To assess the methodological quality of the studies, two critical appraisal tools from the Center for Evidence-Based Management (CEBMa) were used: (1) *Checklist for Qualitative Studies* [41]; and (2) *Checklist for Cross-Sectional Studies (Surveys)* [42]. The appraisals were done by one reviewer and checked by the group.

3.3.3. Reporting results

This paper reports the results of the ScR, presenting them in line with the RQs (in Section 3.1.1). The *Synthesis of the Results* is presented in Sections 4.1 and 4.2, including findings on the nature of existing research and the positive and negative aspects of PIAs in practice. The *Critical Appraisal of Primary Research* is provided in Section 4.3, detailing the quality of primary research studies.

3.4. Results of the selection process

Fig. 1 provides an overview of the selection process for this scoping review. An initial total of 746 studies were identified through the search process. The screening process using Rayyan was performed by two reviewers in double-blind mode, resulting in the identification of 60 relevant studies. Only two studies were not accessible through the researchers' institutional libraries. In such cases, we contacted the authors to request the publication but received no responses. After the screening process, 42 papers were initially included in this review. Using Google Scholar, we checked for all the papers that cited the selected studies (i.e., forward snowballing). This process revealed another two studies that the authors deemed relevant. While reading the full texts, we also looked for studies mentioned or referenced in each publication (i.e., backward snowballing). Although four studies were identified through backward snowballing, two of them were not found in any databases (not even the bibliographic entries), and one of them was not accessible, so the authors were contacted, but they were also unable to
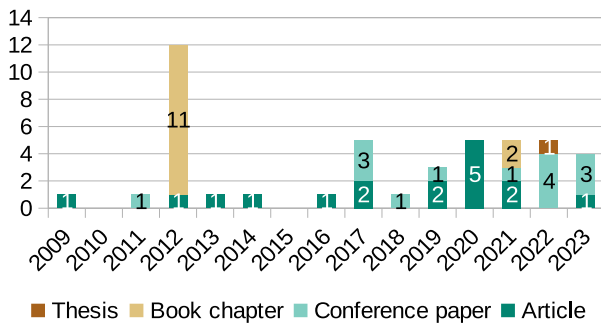
Fig. 2. Publications published per year.

locate the full texts. One additional study was included as part of the backward snowballing process. Finally, 45 studies were included in the ScR (complete list in Appendix B).

4. Results

In this section, the results are organised according to each of our RQs. First, RQ1 is addressed in Section 4.1 by presenting the nature of the literature and evidence of the topic, describing several demographics of the selected studies. The results related to RQ2 are presented in Section 4.2, describing the main PIAs methodologies and a thematic framework of the positive and negative aspects in practice. Lastly, concerning RQ3, the identified primary research studies are critically appraised in Section 4.3.

4.1. The nature of evidence on the topic

4.1.1. Frequency, types of research, and contributions

The following subsections aim to answer RQ1 by describing the key characteristics of the studies included in the ScR, with Fig. 2 showing the numbers and types of publications per year. The studies were categorised using the classification schemes for research types proposed by Wieringa et al. [37] and Creswell and Creswell [38]. As shown in Fig. 3(a), Primary Research is the main type of research with 66.7% of the studies of a qualitative or quantitative nature — primary research studies are further analysed in Section 4.3. The second most common type of research is Experience Papers (37.8%). Such studies describe an author's first-hand experience with dealing with PIAs in specific jurisdictions (e.g., Australia [43] and the UK [44]), private organisations (e.g., Nokia [45], Siemens [46], and Vodafone [47]), or for specific projects (e.g., a data sharing platform [48], the BIRO project [49]). Many studies (28.9%) also propose new solutions, such as suggesting new or enhanced PIA frameworks and processes [9,23,50–54]. Evaluation Research remains incipient, with only a few studies proposing new methodologies performing their practical evaluations (i.e., [50–52,54]), while other studies evaluate public PIA reports and documents [43,55,56], or the use a specific PIA methodology (i.e., CNIL PIA tool in [57–59]).

It is important to clarify that six studies were also classified as Literature Reviews since their authors explicitly mentioned it as part of the objectives (i.e., [9,23,49,60–62]). However, these studies have neither performed systematic reviews as part of their research nor addressed the topic of PIAs "in the wild". Another clarification refers to the studies classified as Opinion Papers. These studies present personal opinions of PIAs in practice primarily based on first-hand experience and without relying on related work or research methodologies (i.e., [7, 63–65]). Although some types of systematic review methodologies would exclude such types of publications, ScRs purposefully include such studies since they seek to map a research area comprehensively, as discussed in [34].

For the contribution types, studies were categorised using the classification proposed by Shaw [39]. As shown in Fig. 3(b), most studies (77.8%) contributed with Lessons Learnt drawn from their results. Five studies (11.1%) also contributed with Frameworks, that is, PIA frameworks or methodologies [50–54], and seven studies (15.6%) with various kinds of Models (e.g., PIA process model [9], system model [49], threat and control models [66,67], or a typology [60]).

4.1.2. Countries and publication venues

By reviewing the affiliations of the authors of the included studies, we found that 12 studies (26.7%) came from the United Kingdom, followed by Germany with five studies (11.1%), the Netherlands and Italy with four studies each (8.9%), and the United States, Belgium, Australia and France with three studies each (6.7%). Institutions of 14 other countries were accounted for in the studies but with only two or fewer publications. Besides, the publications come from a heterogeneous number of venues, with 32 studies published in various conference proceedings, journals, or as doctoral theses. Eleven studies are chapters of the book [68], and two studies come from the journal of *International Data Privacy Law*.

4.1.3. Industry sectors, laws and regulations

During the data extraction stage, relevant information concerning the application context of the studies was captured, generating a classification for types of organisations, as shown in Fig. 4. Most studies (42.2%) were applied to Public Sector organisations, such as studies focused on PIA processes in government agencies [8,56,63], public health and healthcare institutions [51,65,69], or national security and police agencies [43,67,70,71]. Many studies (26.7%) were not focused on a specific context, addressing the topic of PIAs more broadly and involving various stakeholders and practitioners, such as Ferra et al. [72], Vandercruysse et al. [60], Vandercruysse et al. [73], Wright et al. [74] and Schneider et al. [23]. The private sector was represented in 10 studies (22.2%), such as in reports from Nokia [45], Vodafone [47], Siemens [46], among other sectors, for instance banking [61], medical device manufacturers [9], telecommunications [59], and mobile app companies [11].

Regarding privacy laws and regulations, the studies collectively mention many legal references, but the most commonly mentioned is the EU GDPR (60%), as shown in Fig. 5(a). Other privacy regulations were mentioned to a lesser extent, such as the EU Data Protection Directive (17.8%) that preceded the EU GDPR, and the OECD privacy principles (6.7%), among others.

4.2. The scientific reports on PIAs in practice

4.2.1. PIA frameworks

Many PIA frameworks (i.e., full-fledged methodologies or guidelines) that are mentioned or used in the studies were also identified. As shown in Fig. 5(b), the most popular PIA framework was the one from the UK Information Commissioner's Office, which was mentioned in 17 studies (37.8%). Other well-known PIA frameworks were also mentioned: the French PIA Methodology [16] (17.8%) from the Commission nationale de l'informatique et des libertés; the Australian PIA Guide [17] (15.6%) from the Office of Australian Information Commissioner; the New Zealander PIA Handbook [13] (13.3%) from the Office of the Privacy Commissioner; the German PIA guidelines [14,15] (13.3%) provided by the Bundesamt für Sicherheit in der Informationstechnik and based on the work of Oetzel and Spiekermann [25]; and the ISO/IEC 29134 Guidelines for PIAs [18] (8.9%). Several PIA frameworks were categorised as Other (46.7%) since they were mentioned in only three or fewer studies.

Among the selected studies in this ScR, eight publications introduced a novel PIA or DPIA methodology/framework as part of their research (see Table 1). In 2013, the work of Wright and Wadhwa [75] introduced the Privacy Impact Assessment Framework (PIAF).
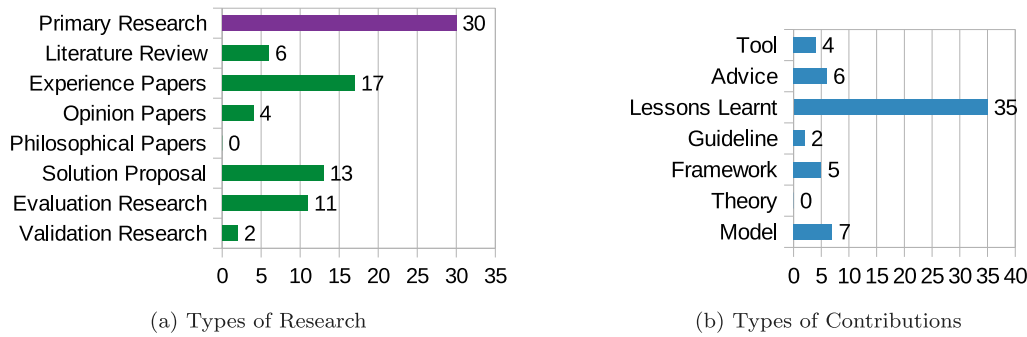
(a) Types of Research   (b) Types of Contributions

Fig. 3. Chart (a) number of studies categorised by Research Types. Chart (b) number of studies for different types of contributions.

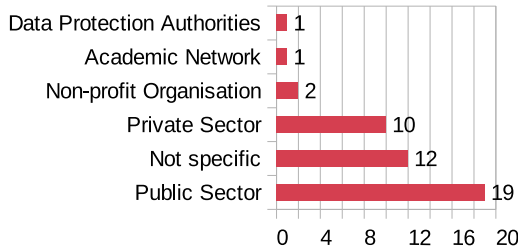**Fig. 4.** Types of organisations.

Table 1
Studies that introduced new PIA/DPIA methodologies or frameworks.

New methodology	Ref.
PIA by model-based privacy analysis	Ahmadian et al. [50]
Privacy impact assessment framework	Wright and Wadhwa [75]
DPIA methodology for healthcare systems	Todde et al. [51]
DPIA data wheel methodology	Henriksen-Bulmer et al. [52]
Agile E/PIA methodology	Kroener et al. [53]
DPIA framework	Friedewald et al. [54]
Privacy assessment methodology model	McKee [9]
Persona-oriented DPIA for SMEs	Schneider et al. [23]

Table 2
Studies that adopted an existing PIA methodology or framework.

Methodology	Ref.
CNIL PIA	Campanile et al. [57], Rajamäki [70], Dashti et al. [77] and Alaqra et al. [58]
PAPAYA PIA tool	Alaqra et al. [59]
BSI/RFID PIA	Iwaya et al. [66]
UK ICO PIA	Wright et al. [74]
AU OAIC PIA	Pribadi and Suryanegara [78]

The other seven studies, published between 2018 and 2023 (after GDPR came into effect), proposed other solutions, such as the PIA by model-based privacy analysis [50] and the persona-oriented DPIA [23]. Also, eight studies describe their use and experience with existing PIA frameworks, as shown in Table 2. The most used methodology among these studies is the CNIL PIA tool, which was also used as a basis for the PAPAYA PIA Tool discussed in [59,76].

Apart from that, five studies have described *ad-hoc* or "in-house" PIA methodologies that were used in their organisations. For instance, the works of Horák et al. [48], Iorio et al. [49], and Bas Seyyar and Geradts [71] describe the conduction and experience with PIAs that were devised based on existing regulations and applied *ad-hoc* in their specific projects. Other industries describe their in-house PIA approaches, such as Nokia's privacy impact and security assessment (PISA) template [45] and Vodafone's Strategic PIA as part of their privacy risk management system.

4.2.2. On the positive and negative aspects of PIAs in practice

This subsection focuses on answering RQ2 concerning the positive and negative aspects of PIAs in practice, as reported in the ScR studies. Fig. 6 shows an overall picture of the main aspects identified by the authors from reviewing the studies. Even though such aspects come from the authors' efforts to synthesise the content, it is worth stressing that this list is not meant to be an exhaustive enumeration of aspects but rather to be seen as a high-level overview. The aspects are numbered in order of prevalence, that is, the aspect is covered in more studies; however, this should not be interpreted as a prioritisation or ranking of importance. As part of the replication package [36], a summary of the generated codebook is provided as supplementary material, containing exemplary quotes and references that helped us form each sub-theme. A compilation of positive (P) and negative (N) aspects is presented in what follows.

P1 — Ethics, Legal Compliance, Communication with Regulators

Starting with the positive aspects, the identified sub-themes are distributed over a total of 43 studies, as shown in Fig. 7. Most studies stressed the benefits of **PIAs for meeting regulatory compliance** when developing or deploying systems. PIAs are regarded as established risk analysis methodologies that enable organisations to pursue their commercial strategies whilst satisfying people's privacy expectations and **meeting legal and ethical obligations** [47]. In addition, it was also often mentioned that PIAs can be leveraged to better communicate with regulators (e.g., DPAs or privacy commissioners). PIAs can act as **accountability mechanisms in the review or audit of implemented mitigation measures** [7], facilitating the investigations for regulators. At the same time, organisations can use the PIAs and documented processes for **demonstrating compliance with regulators**, data subjects, and platform users [48]. Ultimately, proper PIAs can be used as **a basis for discussion with regulators** as well as other stakeholders (e.g., researchers, journalists, civil societies, the general public) [69].

P2 — PIA best practices and recommendations

Several best practices and recommendations for high-quality PIAs were reflected in the studies. Among them, it is essential to understand **PIAs as processes and living documents** that should be iteratively refined whenever privacy objectives shift in the system design [71], and periodically reviewed for changes of assumptions or when new privacy threats are discovered [66]. PIAs are only effective if their outcomes can be realised, so it is also important to **start early to maximise results** when project changes are still feasible. At an early stage, the project team can consider warnings in the PIA, allowing them to rethink the design, focusing on purposeful features that are less privacy-invasive [79]. Similarly, if an organisation is acquiring new information systems, PIAs can better inform the project team if performed before the deployment process in the real environment [51].

Practitioners also argued that in order to be effective, PIAs need to **define the scope of analysis and limitations** with proportional depth to many crucial variables, such as the size of the organisation,

(a) Privacy Regulations
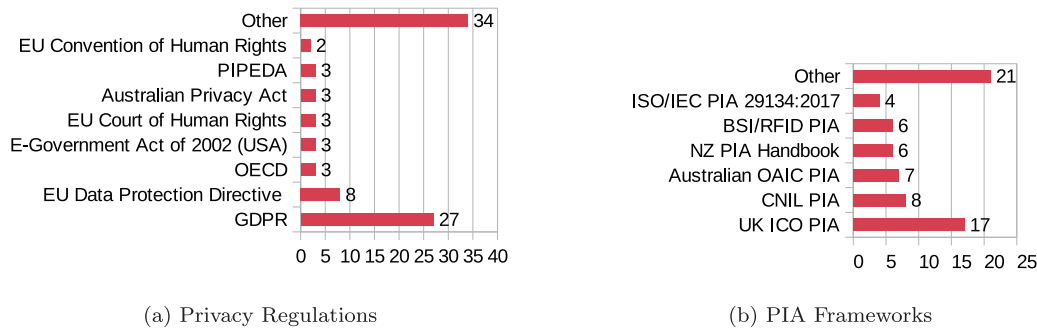
(b) PIA Frameworks

Fig. 5. Chart (a) most mentioned privacy regulations, and chart (b) most mentioned PIA/DPIA frameworks and methodologies.
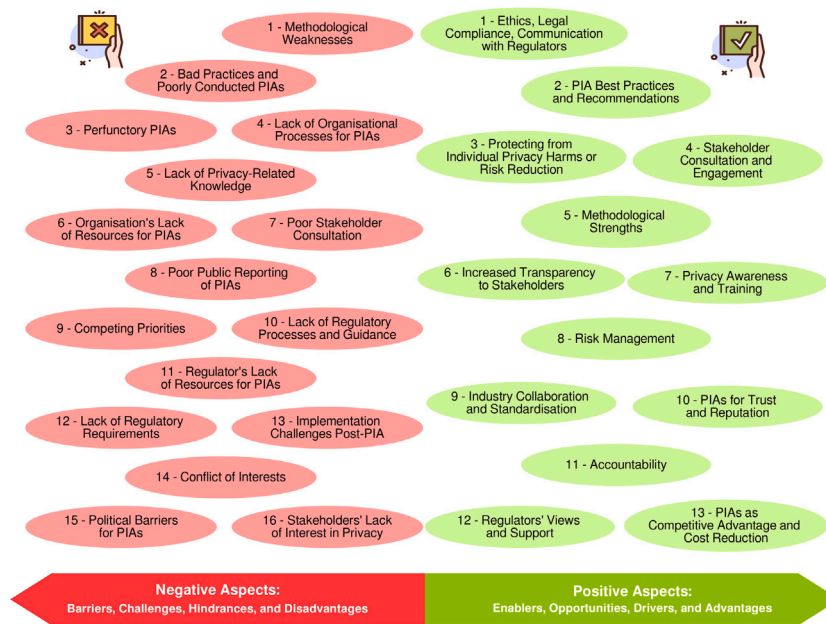
Fig. 6. An overview of the sub-themes on the positive and negative aspects related to PIAs in practice as reported in the studies.

sensitivity of the data and processing operations, forms of risks and intrusiveness of the technology [44]. The scope constraints of the project must be clearly described, and the PIA report should only account for such precise descriptions, protecting assessors from potential scope creep in the future [6].

Another strong recommendation by practitioners is to ensure the **independence of privacy experts and assessors**, whether they are internal (e.g., privacy officers, experts, hired consultants) or external (e.g., regulators) to the organisation. Regulators clearly have an obligation to be independent of the organisations since they represent the public interest and are expected to protect the community [64]. More importantly, the internal representatives in the organisation responsible for the assessment should also have enough independence so that when highlighting challenges, legal limitations, and risks, their assessment cannot be simply overturned or dismissed by other members [46]. Practitioners also emphasised the importance of **developing a strong process for PIAs**, with proper scoping and project management methods for handling the assessments in a sensible and efficient manner [73].

Finally, practitioners indicated that they can **reuse and share past PIAs, tools, and catalogues** to help others inside or outside the organisation. Those conducting large numbers of PIAs can compile supporting materials of common privacy risks and mitigation strategies, improving the efficiency of future PIAs and accumulating knowledge

within the organisation [7]. Nonetheless, it is also possible to take advantage of well-maintained catalogues of privacy threats and controls that supervisory authorities have already created [54], for instance, CNIL's PIA templates [80] and knowledge bases [81].

P3 — Protecting Individuals from Privacy Harms and Risk Reduction

Several studies described using **PIAs for better privacy, minimising privacy harms by identifying threats and appropriate controls** with the ultimate focus on the data subjects. PIAs helped in visualising impact levels (e.g., matrices for risk likelihood and severity), raising awareness among developers and finding better ways to handle personal data [57]. They also compel project members to justify the data collection and processing operations, balancing risks, costs for implementing controls, and resulting benefits [53]. In doing so, PIAs bridge a gap between legal principles and engineering practices by providing a systematic way of identifying risks and controls, giving developers a clearer path towards solving privacy issues and protecting individuals [66].

P4 — Stakeholder consultation and engagement

High-quality PIAs require good consultation with both **internal** and **external** stakeholders. Among the internal stakeholders, **senior and privacy experts** with diverse disciplinary skills can be involved, or

Fig. 7. Overview of studies distributed across the sub-themes of positive aspects related to PIAs in practice.

Column headers (studies):
Alagra et al. (2021), Alagra et al. (2023), Bamberger and Mulligan (2012), Bas Seyyar and Geradts (2020), Bayley and Bennet (2012), Brautigam (2012), Campanile et al. (2022), Clarke (2016), Dashti et al. (2021),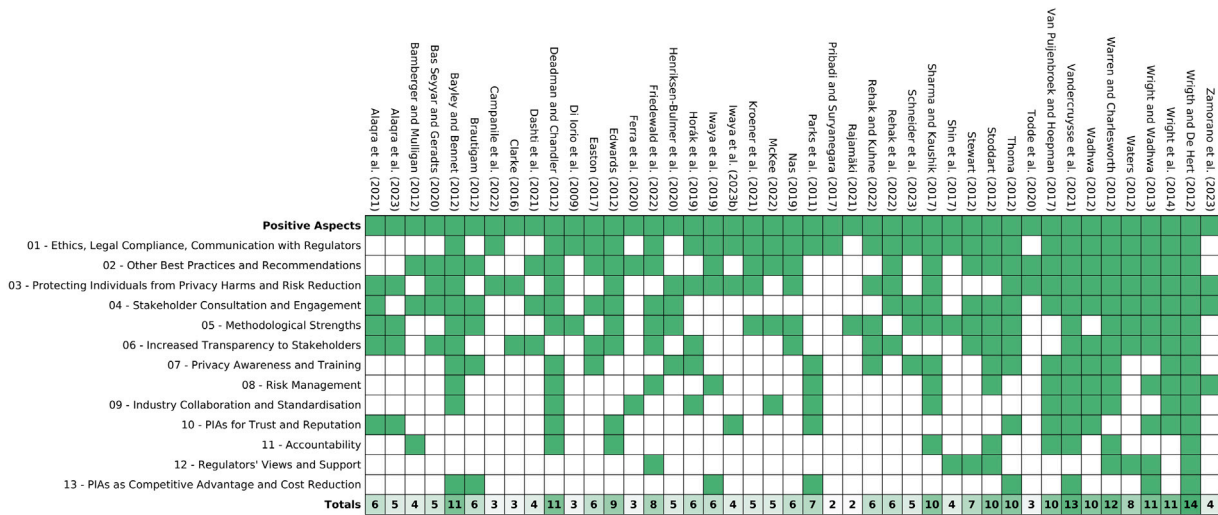 Deadman and Chandler (2012), Di Iorio et al. (2009), Easton (2017), Edwards (2012), Ferra et al. (2020), Friedewald et al. (2022), Henriksen-Bulmer et al. (2020), Horák et al. (2019), Iwaya et al. (2019), Iwaya et al. (2023b), Kroener et al. (2021), McKee (2022), Nas (2019), Parks et al. (2011), Pribadi and Suryanegara (2021), Rajamäki (2021), Rehak and Kuhne (2022), Rehak et al. (2022), Schneider et al. (2023), Sharma and Kaushik (2017), Shin et al. (2017), Stewart (2012), Stoddart (2012), Thoma (2012), Todde et al. (2020), Van Puijenbroek and Hoepman (2017), Vandercruysse et al. (2021), Wadhwa (2012), Warren and Charlesworth (2012), Waters (2012), Wright and Wadhwa (2013), Wright et al. (2014), Wright and De Hert (2012), Zamorano et al. (2023)

Row sub-themes (Positive Aspects):
- 01 - Ethics, Legal Compliance, Communication with Regulators
- 02 - Other Best Practices and Recommendations
- 03 - Protecting Individuals from Privacy Harms and Risk Reduction
- 04 - Stakeholder Consultation and Engagement
- 05 - Methodological Strengths
- 06 - Increased Transparency to Stakeholders
- 07 - Privacy Awareness and Training
- 08 - Risk Management
- 09 - Industry Collaboration and Standardisation
- 10 - PIAs for Trust and Reputation
- 11 - Accountability
- 12 - Regulators' Views and Support
- 13 - PIAs as Competitive Advantage and Cost Reduction

Totals: 6, 5, 4, 5, 11, 6, 3, 3, 4, 11, 3, 6, 9, 3, 8, 5, 6, 6, 4, 5, 5, 6, 7, 2, 2, 6, 6, 5, 10, 4, 7, 10, 10, 3, 10, 13, 10, 12, 8, 11, 11, 14, 4

preferably, embedded within operational units of the organisation, taking advantage of the interdisciplinary nature of PIA tools for generating "bottom-up" decision-making [63]. PIA practitioners can also leverage internal **collaboration cross-teams and with domain experts**, learning from experience across departmental boundaries and getting directly involved with developers and main internal users. The collaboration between developers, domain experts, and PIA practitioners is crucial in the threat elicitation process and helps raise privacy awareness in the teams [71]. Another important internal aspect is getting **management support** throughout the PIA process, that is, "buy-in" from senior management, also developing a culture of privacy within the organisation [74]. Similarly, **engaging project members** was also regarded as crucial, that is, ensuring that people involved do not see the PIA as a constraining exercise or a legal obstacle and, instead, focus on the wider PIA benefits such as transparency, confidence, and process streamlining that can directly benefit the project, the system under development, or the organisation [82].

A significant part of the PIAs also involves **engaging with external stakeholders** that can help to inform, seek agreement, and provide feedback on the policies of the organisation [47]. More specifically, it is of utmost importance to leverage **public consultations and involve data subjects** (or their representatives) as a thorough basis for assessing privacy risks, seeking heterogeneous views [54]. Studies also recognised the expertise of the regulators and the usefulness of **external PIA reviews** and feedback, in which organisations can seek comments to further understand and manage privacy risks to deliver good privacy outcomes to individuals [64].

P5 — Methodological strengths

PIA frameworks are often acclaimed for their methodological strengths. Some consider **PIAs as a privacy-by-design approach** since the methodologies offer a general solution to build robust privacy-protective information systems [49]. The **continuous improvement and streamlining of PIA frameworks**, methodologies, and software tools have also made PIA more practical and improved collaboration among practitioners and other stakeholders [70]. Security researchers also refer to **PIAs as systematic and sound methodologies for risk analysis** that can be used for rigorous evaluation of systems, and final reports can be disseminated for public scrutiny [69]. Throughout the years, **PIAs have been considered a widespread practice** [7,8], being commissioned and prepared in a wide range of initiatives and innovation proposal [6], which has also helped to establish the methodology among practitioners and policymakers.

P6 — Increased transparency to stakeholders

Using **PIAs for increased transparency** was also reported as a key advantage. As noted by Clarke [43], the conduct of proper PIAs has the benefit of forcing a degree of transparency, enabling informed decision-making by stakeholders that can more easily identify privacy issues and impose appropriate controls. To achieve higher levels of transparency, **publishing the public PIA reports** of systems has also been suggested as a way to deal with privacy concerns through public debate. In this way, it is also possible to use **PIAs as a basis for societal discussion of privacy risks**, enabling the informing and involvement of the media, political parties, and the broad population [83]. Nonetheless, such public PIA reports should be made easily accessible instead of having them buried on a website. An alternative is to **leverage central PIA repositories** that could be managed by a supervisory authority [62].

P7 — Privacy awareness and training

It has been reported that companies can use the **PIA self-assessment for increased privacy awareness in the organisation**, especially when using contextual questions as part of the PIAs, clarifying the meanings of privacy risks and its nuances in a specific context [52]. Some studies also discussed the link between **PIAs and the organisational privacy culture**, emphasising the benefits of proactive approaches to ensure privacy, such as the annual refresh of PIAs, trigger-based updates, and promoting a privacy culture [61]. In addition, organisations should **ensure that staff has PIA and privacy training**. Specialised PIA training and basic privacy training can help bridge knowledge gaps in the organisation by equipping more professionals to participate in PIAs instead of stretching the resources of a few qualified staff [7].

P8 — Risk management

Many studies have highlighted the need to integrate **PIAs as part of the risk management process** [74]. The organisational risk management approach can readily use PIA frameworks as effective tools for assessing different types of privacy risks [84]. Furthermore, the use of **PIAs helps to identify the people responsible for treating issues and risks in the organisation**. Whilst seeking agreement and prioritising actions, the PIA process also brings up the discussion on the correct people within business units that are responsible and can effectively treat privacy risks (i.e., the privacy risk owners), which are likely to be different from privacy officers of managers [47].

P9 — Industry collaboration and standardisation

Industry practitioners **sharing PIA experience and tools with others outside the organisation** were found to be a positive aspect for increasing knowledge levels and confidence in PIA practices [72]. Studies have shown that many **industry professionals see benefits and plan to use PIAs** once they receive basic training on the methodologies [9]. Standardisation initiatives have also helped to establish PIA frameworks in the industry further, for instance, ISO/IEC 29134:2023 [18].

P10 — PIAs for trust and reputation

Organisations can also leverage **PIAs for building trust and reputation**, using them as a foundation of their broader privacy strategies [47]. A strong reputation for privacy helps companies garner citizens' trust, especially when they publish PIA reports, showing more transparency and allowing business associates to judge procedures on a more technical level [73].

P11 — Accountability

When adopting PIA practices, it is critical that organisations **develop mechanisms for accountability, monitoring, and internal or external oversight** to see benefits to their full potential, as advised by scholars and policymakers [63]. For instance, a mechanism or strategy includes the signing off of the PIA report by critical parties, such as, project owners, line managers, privacy and security officers, or executives [8,12,61]. This approach improved the involvement of the key parties and the quality of the PIA reports [12].

P12 — Regulators' views and support

Some studies reported that support and **clearer guidelines for PIAs from data protection supervisory authorities are helpful**, allowing practitioners to have more precise and clear explanations [54]. An example is the guideline that further explains the notion of data processing operations with "high risk" to the rights and freedoms of individuals [19], therefore providing clearer criteria for assessors. Studies focused on the Data Protection Authorities (DPAs) also indicate that the **regulators play a strong advocacy role** in ensuring that PIAs are properly done, that they are independently reviewed, and that safeguards are implemented, thus impacting the citizens' and consumers' trust in organisations [75].

P13 — PIAs as competitive advantage and cost reduction

Even though privacy requires significant investments from organisations, experts mostly agree that **the benefits of a PIA far outweigh the costs** [45,75]. As a privacy-by-design strategy, PIAs allow issues to be identified at the conception stage when design changes are significantly simpler and less costly if compared to later stages of software development (such as testing and deployment) [66]. For many organisations **PIAs and privacy are seen as a competitive advantage** [7], differentiating them from competitors through higher levels of privacy and data protection [84] and demonstrating that their products are safe [60].

N1 — Methodological weaknesses

Moving to the negative aspects of PIAs in practice, the identified sub-themes are distributed over a total of 39 studies, as shown in Fig. 8. Several studies stressed the **inherent challenges of risk assessments** that also apply to PIA methodologies. Risk assessments elicit privacy threats and calculate the likelihood and severity of risks, which are based on the description of the system and the best knowledge of practitioners. In turn, this creates a shifting ground for PIAs, especially when assessing new and innovative technologies that may be used for unforeseen purposes and circumstances [82]. As discussed in [66,85], the estimation of risk in a mathematical sense is never complete, every possible undesired event (threat) is never known, and countermeasures for new attacks and vulnerabilities may not exist yet, so assessments always need to be continuously revised.

Another barrier that practitioners express is that **PIA methodologies need to be streamlined or are too complicated and complex**. As reported in [74], many consider PIA frameworks "not business friendly", "too onerous", or "too dense and complex", deeming them unsuitable to support the objectives of the company. Other studies proposing new PIA methodologies also faced criticism, in which industry experts perceived the methodologies as trying to do too much and no longer being simple and easy to follow [9].

Some studies also criticised the **low credibility or proven effectiveness of PIA-related methods**, pointing to the limited evidence to indicate that PIAs are really attaining their stated goals in an efficient and cost-effective manner [54,55]. Coupled with that, practitioners also see deficiencies in terms of the **subjectivity** of the risk analysis processes. For many, the risk analysis is not only dependent on the skills and experience of the person doing the assessment, but deriving privacy risks (e.g., estimating likelihood and severity levels) is also perceived as a vague task [12].

N2 — Bad practices and poorly conducted PIAs

Among the most common bad practices, the **inconsistent conduction of PIAs** was often reported, characterised by a lack of processes and clear responsibilities. For example, the privacy officer's irregular involvement in the product and service development processes of the organisation would also lead to PIAs being conducted inconsistently [47]. Another major issue is the lack of planning with PIAs being carried out without a thought-out process [73]. Other organisations attempt to create their own PIA process but lack a systematic and comprehensive methodology that would enable them to fulfil regulatory requirements (e.g., GDPR) [65].

The problem with **insufficient information for doing PIAs** was also reported, evidenced by the lack of documentation for the analysis [45]. The PIA preparation phase would often reveal such issues, showing how incomplete the knowledge of those in charge was when discussing the details and context of data processing operations [54]. Such problems would also result in **inappropriate risk analysis**, overlooking threats and risks, especially for scenarios beyond the normal processing activities, for instance when law enforcement gains access to data [54]. Another common issue in risk analysis is the **disregard for data subjects**, with organisations focusing on organisational risks instead of the risk to their customers or other individuals [52,72]. This was also the case when dealing with risks to internal data subjects, for instance employees, seen as low priority [54].

N3 — Perfunctory PIAs

PIAs are also reported to be conducted on a perfunctory basis [55], that is, done merely out of duty with little interest or care. The issue of **ceremonial or *pro forma* performance of PIAs** has been linked to external mandates, where organisations adopt PIAs to appear legitimate but actually minimising the changes of existing practices and priorities [63]. Practitioners have also reported that PIAs are often completed as a standard practice and then "put on a shelf" just to be referenced as a metric [72].

Reports further show that **PIAs were conducted *ex post facto* or when it was already too late**, and changes were limited and costly [8]. Late PIAs have marginal utility once the design parameters of the project have been set, an organisational structure is committed, and major costs incurred [79]. Practitioners have criticised such approaches, considering that organisations misunderstand the purpose of PIAs or might seek to mischaracterise them [86].

N4 — Lack of organisational processes for PIAs

Aspects such as the **lack of management support and infrastructure for PIAs** are considered barriers. The organisational process for managing PIAs needs to be defined and implemented, supported by specific actors in charge of maintaining and updating the documentation and produced assessments [51]. Furthermore, creating and sustaining
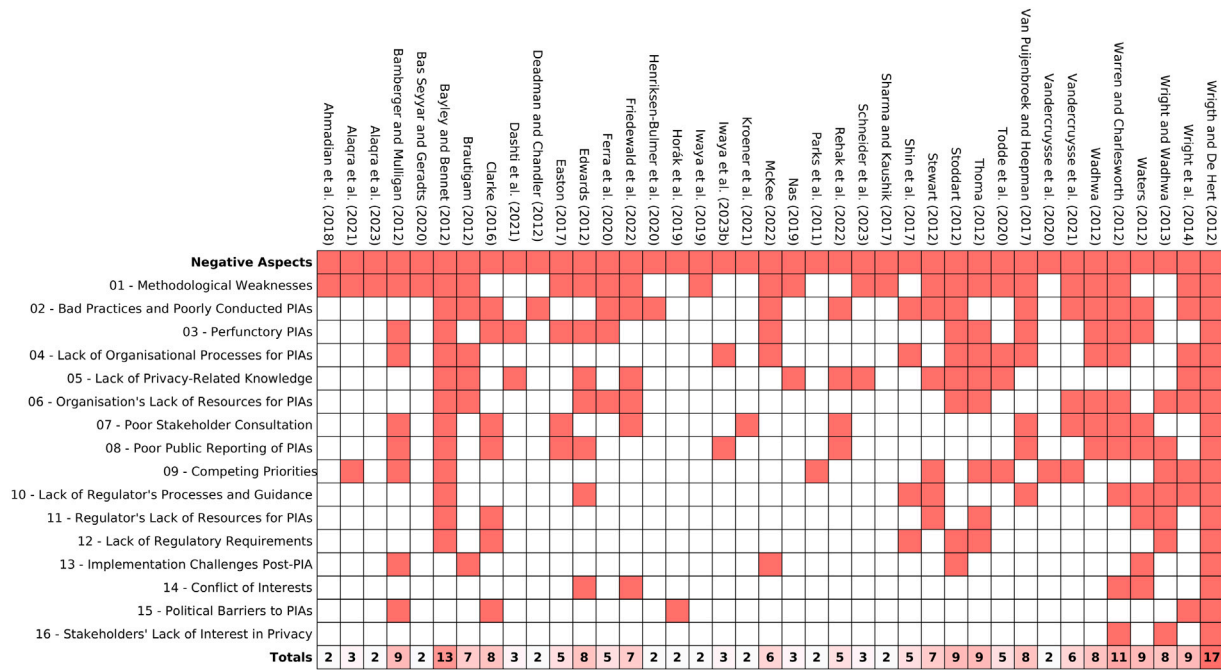
Negative Aspects (columns: Ahmadian et al. (2018); Alagra et al. (2021); Alagra et al. (2023); Bamberger and Mulligan (2012); Bas Seyyar and Geradts (2020); Bayley and Bennet (2012); Brautigam (2012); Clarke (2016); Dashti et al. (2021); Deadman and Chandler (2012); Easton (2017); Edwards (2012); Ferra et al. (2020); Friedewald et al. (2022); Henriksen-Bulmer et al. (2020); Horak et al. (2019); Iwaya et al. (2019); Iwaya et al. (2023b); Kroener et al. (2021); McKee (2022); Nas (2019); Parks et al. (2011); Rehak et al. (2022); Schneider et al. (2023); Sharma and Kaushik (2017); Shin et al. (2017); Stewart (2012); Stoddart (2012); Thoma (2012); Todde et al. (2020); Van Puijenbroek and Hoepman (2017); Vandercruysse et al. (2021); Vandercruysse et al. (2020); Wadhwa (2012); Warren and Charlesworth (2012); Waters (2012); Wright and Wadhwa (2013); Wright et al. (2014); Wrigth and De Hert (2012))

Rows:
- 01 - Methodological Weaknesses
- 02 - Bad Practices and Poorly Conducted PIAs
- 03 - Perfunctory PIAs
- 04 - Lack of Organisational Processes for PIAs
- 05 - Lack of Privacy-Related Knowledge
- 06 - Organisation's Lack of Resources for PIAs
- 07 - Poor Stakeholder Consultation
- 08 - Poor Public Reporting of PIAs
- 09 - Competing Priorities
- 10 - Lack of Regulator's Processes and Guidance
- 11 - Regulator's Lack of Resources for PIAs
- 12 - Lack of Regulatory Requirements
- 13 - Implementation Challenges Post-PIA
- 14 - Conflict of Interests
- 15 - Political Barriers to PIAs
- 16 - Stakeholders' Lack of Interest in Privacy

Totals: 2, 3, 2, 9, 2, 13, 7, 8, 3, 2, 5, 8, 5, 7, 2, 2, 2, 3, 2, 6, 3, 2, 5, 3, 2, 5, 7, 9, 9, 5, 8, 2, 6, 8, 11, 9, 8, 9, 17

Fig. 8. Overview of studies distributed across the sub-themes of Negatives Aspects related to PIAs in practice.

such PIA infrastructures will be difficult without strong senior management support [7,8]. The lack of a holistic privacy assessment process has also led many practitioners to report that **PIAs are not being carried out** in their organisations [9]. And when PIAs are conducted, it is common to see a **lack of internal audit evaluation processes**, with little or no auditing of the PIAs performed in practice [12].

N5 — Lack of privacy-related knowledge

Practitioners mentioned the lack of privacy-related knowledge as one of the obstacles to implementing PIA practices. For instance, **confusing privacy with security and confidentiality** and failing to recognise the boundaries between concepts would result in misjudgements about the necessity of a PIA or privacy impacts to data subjects [77]. Another example is the **confusion or uncertainty about the roles of data processors and joint data controllers**, especially for organisations that operate in an ecosystem with several global service providers and 3rd parties [83]. The lack of knowledge about PIAs also requires practitioners to **clearly explain and set expectations to clients** regularly, clarifying what the assessment is intended to do and is capable of delivering [6].

N6 — Organisation's lack of resources for PIAs

Sometimes, organisations pointed to a lack of various types of resources needed for conducting PIAs. The **lack of PIA expertise or experts** was among the greatest difficulties encountered by some organisations, finding it hard to locate experienced practitioners outside the organisation [44], let alone identify internal people with such knowledge. Practitioners also pointed to an alleged **lack of resources for conducting PIAs**, with typical arguments such as missing resources, expected delays, additional costs, lack of need, and reluctance to start the process [46]. To some extent, even some DPAs have acknowledged that **PIAs are seen as a burden or a hurdle** and that the costs may be prohibitive for companies and agencies that do not have the financial capacity, incurring in seemingly unnecessary costs [55].

N7 — Poor stakeholder consultation

A challenge to the proper conduct of PIAs refers to the **lack of mechanisms for public participation or consultation**, limiting opportunities for outside experts to assist in assessing complex technological systems [63]. This issue has also been linked to a methodological

deficiency of popular PIA frameworks that lack concrete guidance or sufficiently describe citizen involvement processes [73]. Practitioners wrote that sometimes **public participation is obstructed and suggestions are ignored**, such as precluding the participation of advocacy groups or limiting comments to a rather late stage in the project, for instance after legislation is drafted and tabled [43].

N8 — Poor public reporting of PIAs

A negative aspect of transparency is the poor public reporting of PIAs, both from the public sector and from the private sector. For governmental institutions, **PIAs are not made available to the public**, or they are not easy to access, hidden on the websites of agencies without clear links; and for private companies, public PIAs are almost non-existent [55]. Organisations also reported fears and barriers to releasing public PIAs, including concerns about the sensitivity of data and systems and the obstruction of self-criticism since participants would feel more guarded if subjected to a public open process [82].

N9 — Competing priorities

The clash with other organisational priorities was also a significant hindrance for PIAs in practice. Project budgets are affected since **PIAs can incur extra costs and delays**, putting especially start-ups, small- and medium-sized companies at a disadvantage [55]. Some practitioners also emphasised that meaningful engagement with **PIAs may disrupt the internal workings of an organisation** [63]. Although this may be the exact purpose of PIA mandates, that is, forcing substantive change in the face of privacy-invasive operations, the internal reorientation process can be challenging. In general, stakeholders think that the central functions of a service are to be kept and that privacy considerations should not unnecessarily impede business goals [73].

N10 - Lack of regulatory processes and guidance

The absence of some regulatory processes was also discussed in the following studies. Regulatory challenges such as the **lack of mechanisms in the government for accountability of the implementation of PIAs plans** and promised mitigation measures were criticised by industry consultants [7]. Other practitioners notice that **there is no**

central registry of PIA reports, and there are no requirements to share reports with regulators or publish them anywhere [6]. This adds to the opacity of the PIA processes in practice, making it hard to understand the uptake and evaluate the effectiveness of PIAs by the public and private sectors.

N11 - Regulator's lack of resources for PIAs

Similar to companies, there is a **lack of resources for PIA-related activities on the regulator's side**. In practice, regulators are unlikely to receive enough resources for in-depth audits or to adequately supervise organisations and directly engage with several PIA project proponents [79]. Adding to the problem, changes in government and political disputes have also been used to **undermine regulatory agencies** by denying funding or obstructing their work [43].

N12 - Lack of regulatory requirements

Given that **PIAs were not mandatory for the public or private sector** in many jurisdictions, institutions often would not conduct them [46]. This lack of an explicit legal requirement and unified form and method leaves PIAs to be conducted based on the controller's discretion and goodwill, which is not always present when it comes to respecting privacy rights [75]. Although the EU has made PIAs mandatory when processing operations are *"likely to result in a high risk to the rights and freedoms of natural persons"*, as stated in Article 35 of the GDPR [3], in many countries, PIAs are still not a legal obligation but only "encouraged" [87].

N13 - Implementation challenges post-PIA

Practitioners have highlighted **the challenge of implementing the identified measures after completing the PIA**. A core challenge is to have a supporting structure to follow up on the implementation status and to make the right people aware of the PIA findings so they can be truly implemented [45]. Some reports further discuss when **PIAs do not bring on actual change in organisational practices**, for instance when clients do not welcome many recommendations, and there is significant tension in the finalisation of the report to mask core issues in the text so that potential critics cannot use the PIA work as effectively [79].

N14 - Conflict of interests

A critical factor that can compromise the credibility of PIAs is the **conflict of interests of internal or external assessors**. Practitioners have discussed the challenge of achieving real independence in the PIA process since both in-house staff and consultants doing the PIAs have their livelihood depending on delivering work that pleases rather than annoys those who pay them [6]. The organisation contracts most PIA practitioners and therefore expects them to act in the best interest of the business, making it difficult for them to assess risks in a truly unbiased manner, prioritising the concerns of the data subject [54].

N15 - Political barriers for PIAs

Some political barriers have been more particularly linked to the practice of PIAs within government agencies and in policy-making. As discussed in [63], information abuse in governmental initiatives is also a concern; however, expending political capital on privacy can be considered risky. Furthermore, there is also a clash among the values of **privacy versus efficiency and national security**, in which privacy can be seen as a hindrance for the others [63]. Practitioners also reported other reasons for the **conflicts of PIAs in policy-making**, such as the complexity of this type of work, the involvement of several ministers and bargaining consultations, and the need "to get on" with the policy-making and final deliverables [74].
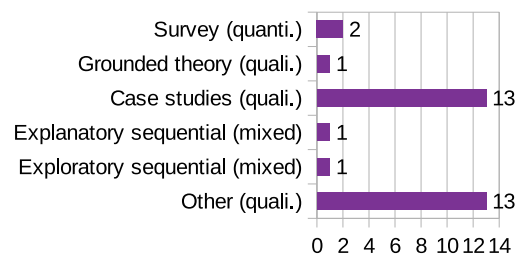
Fig. 9. Types of primary research.

N16 - Stakeholders' lack of interest in privacy

Although stakeholder consultation is an essential part of the PIA process, there are significant challenges in engaging stakeholders and getting them involved. As reported in [44], some PIA initiatives have faced a **lack of interest from stakeholders in participating in the consultation process**; despite sending several invitations to civil society representatives, very few took part in the consultation event and gave little to no meaningful feedback.

N17 - Dealing with the PIA clients or sponsors

Handling the **disagreements on privacy risks between assessors and clients** is another significant challenge in the PIA process. Without compromising the independence of the report, assessors have to analyse trade-offs and be able to judge when to concede and when to make assertive PIA recommendations, knowing full well that they may be accepted or rejected [6].

4.3. The state of existing primary research

4.3.1. Types of primary research

This section addresses RQ3, delving further into the primary research on the topic. As previously shown in Fig. 3(a), two-thirds of the studies were classified as Primary Research ($n = 30$, 66.7%). These studies were further classified using Creswell and Creswell [38] research design categories, as presented in Fig. 9.

Twenty-eight studies (62.2%) adopted a qualitative methodology, with case studies being the most common approach (28.9%). Thirteen studies (28.9%) used other types of qualitative approaches in their research, including interview-based methods [9,23,45,58,60,63, 78], focus groups [23,59,60,67,72], Delphi study [49], descriptive field study [12], and cognitive walk-through [59].

Only four studies (10%) used survey instruments as part of their research methods [73–75,77]. Two studies were found to use a mixed-methods approach, being categorised as Explanatory Sequential [74] and Exploratory Sequential [73], which relied on both quantitative surveys and qualitative interview-based methods. Nonetheless, we argue that there is still an overall lack of primary research on the topic of PIAs in practice, especially in terms of quantitative research.

4.3.2. Critical appraisal of qualitative studies

As summarised in Tables 3 and 4, the quality of the identified primary research studies was critically appraised using the checklists from the Center for Evidence-Based Management [41,42]. Table 3 shows that the vast majority of the qualitative studies clearly defined a research question or objective (Q1) coupled with the use of appropriate methodologies (Q2). The research context was also sufficiently described in almost all studies (Q3).

The main issues for most studies concerned the descriptions of the data collection (Q4–Q5) and the data analysis procedures (Q6–Q7). The data collection was often described briefly, without detailing the number of participants involved, time spent in interviews, procedures for recording and transcribing data, and missing interview guides or lists of questions used. In terms of allowing the data to be inspected

Table 3

Critical appraisal of qualitative research – Checklist for qualitative studies [41]. A full list of questions is found in Appendix A.1.

Author, year and refer.	Res. design	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Horák et al. [48]	Case study	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Ferra et al. [72]	Other	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
Bräutigam [45]	Other	Yes	No	Yes	No	No	No	No	Yes	Yes	Yes
Bamberger and Mulligan [63]	Other	Yes	No	Yes	No	No	No	No	Yes	Yes	Yes
Ahmadian et al. [50]	Case study	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Iorio et al. [49]	Other	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Vandercruysse et al. [60]	Case study, Other	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
Iwaya et al. [66]	Case study	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Wright et al. [74]	Explan. seq.	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Clarke [43]	Case study	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Todde et al. [51]	Case study	Yes	Yes	No	No	No	No	No	No	No	Yes
Parks et al. [84]	Grounded theory	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Pribadi and Suryanegara [78]	Other	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Sharma and Kaushik [61]	Case study	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Warren and Charlesworth [44]	Case study	Yes	No	Yes	No	No	No	No	Yes	Yes	Yes
Henriksen-Bulmer et al. [52]	Case study	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Bas Seyyar and Geradts [71]	Case study	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
van Puijenbroek and Hoepman [12]	Other	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Kroener et al. [53]	Case study	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Campanile et al. [57]	Case study	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Friedewald et al. [54]	Case study	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
Vandercruysse et al. [73]	Explor. seq.	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
McKee [9]	Other	Yes	Yes	Yes	No	No	No	No	Yes	No	Yes
Alaqra et al. [59]	Other	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Zamorano et al. [67]	Other	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Iwaya et al. [11]	Other	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Schneider et al. [23]	Other	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes
Alaqra et al. [58]	Other	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes

Table 4

Critical appraisal of quantitative research – Checklist for cross-sectional studies (surveys) [42]. A full list of questions is found in Appendix A.2.

Author, year and refer.	Res. design	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
Wright et al. [74]	Expla. seq.	Yes	Yes	Yes	Yes	No	No	No	No	No	No	Yes	No
Wright and Wadhwa [75]	Survey	Yes	Yes	Yes	Yes	Yes	n.a.	Yes	n.a.	n.a.	n.a.	Yes	Yes
Dashti et al. [77]	Survey	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No	Yes	No
Vandercruysse et al. [73]	Explo. seq.	Yes	Yes	Yes	Yes	No	No	No	No	No	No	Yes	No

(Q5), it was predictable that most studies would be unable to make their datasets available since they must maintain the participants' anonymity and avoid confidentiality breaches. Procedures for data analysis were also lacking since most studies did not describe the data analysis approach (e.g., grounded theory, thematic analysis), the number of researchers involved in the analysis, and other quality control measures. Regarding the repetition of the analysis steps, only the study of Iorio et al. [49] was considered adequate since the authors use a Delphi panel for generating consensus, thus inherently seeking reliable agreement.

Nonetheless, most studies were deemed to present credible results (Q8) and justified conclusions (Q9). However, it could be argued that the deficiencies of the studies in terms of the descriptions of data collection and analysis can compromise the final credibility of the results. Finally, most studies still present findings that are transferable to other settings (Q10) in the sense that readers can connect elements of the findings, consider and compare them to their own experience or similar situations, and infer that similar results could be achieved.

4.3.3. Critical appraisal of quantitative studies

Considering the results from Table 4, it was found that all studies had focused research questions/objectives (Q1), employed appropriate methods for addressing them (Q2), and sufficiently explained the research context (Q3). Most issues for quantitative studies come from the possible bias when selecting participants (i.e., most just used convenience samples) (Q4), the lack of representativeness of the samples (Q5) and size for statistical power (Q6). The response rate was usually not discussed in the studies (Q7). The studies also did not describe steps for ensuring the reliability and validity of survey instruments (Q8). Statistical analysis was only assessed in one of the studies [77] (Q9), but

none of the studies presented confidence intervals (Q10). Most studies also did not describe potential confounding variables (Q11).

In conclusion, most results from the studies cannot be applied to other organisations in the strong sense of generalisability. The study of Wright and Wadhwa [75] was an exceptional case since the authors conducted a survey study with the Data Protection Authorities (DPAs) of the 27 EU member states. The study sample can be considered representative since 17 out of the 27 DPAs in the EU responded to the survey, indicating an excellent response rate of 63%. This survey [75] was mostly an opinion-based questionnaire (i.e., free-form text responses), so statistical analysis would not apply, yet for some questions, the authors also organised the answers in categories with percentages. Nonetheless, we still consider that, in general, the methodological appropriateness of the quantitative studies lacks sufficient rigour.

5. Discussion

This ScR provides a comprehensive overview of the topic of PIAs in the wild, synthesising the literature and research in the area. In the following subsections, the main findings, challenges, and pathways for future research are further discussed, and the implications for research and practice are also presented.

5.1. PIAs before and after GDPR

Although several countries today have enforced privacy laws, the European GDPR [3] is undoubtedly the legal framework that has motivated most of the existing research on PIA frameworks and methodologies. As previously shown in Fig. 5(a), 27 out of the 45 studies in this ScR have mentioned the GDPR in their text. In fact, a parallel can be drawn between the timeline of the GDPR and the evolution of PIA
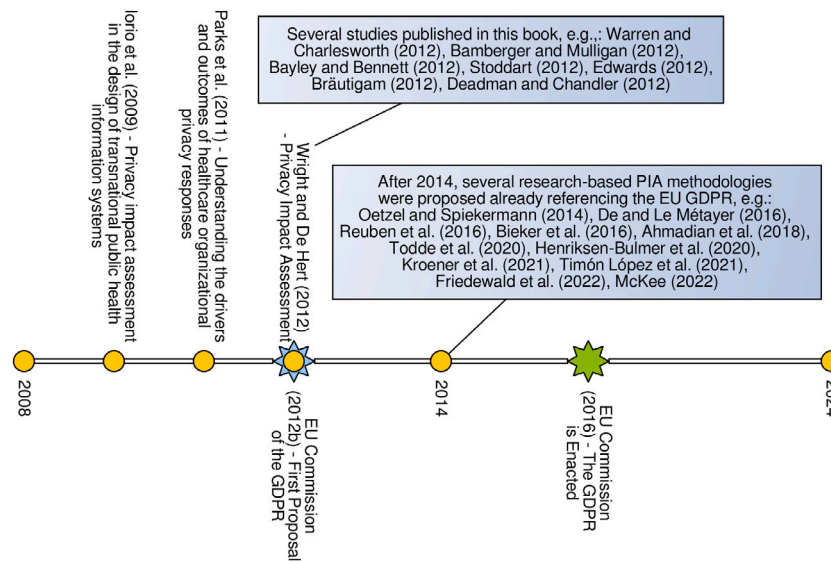
Fig. 10. Timeline overview of the evolution of research on PIAs pre- and post-GDPR.

methodologies, as reflected in the included studies (see Fig. 10). Before 2012, only a few studies had empirically investigated PIAs in practice, such as the works of Iorio et al. [49] and Parks et al. [84]. At this earlier stage, other studies were also primarily pointing to governmental PIA guidelines (e.g., in the UK [44], the US [63], Canada [7,8], and New Zealand [6]) or provided just a quick glance at industry approaches to PIAs (e.g., Nokia [45] and Vodafone [47]).

It was in 2012 that the first proposal of the GDPR was released, which included obligations to data controllers in terms of conducting DPIAs [88]. During 2011 and 2013, more PIA frameworks and methodologies emerged, such as the RFID PIA [15], employing more systematic risk-based methods for identifying threats, associating severity and likelihood levels, and assigning controls [25]. However, most studies ($n = 28$, 62.2%) included in this ScR were published after 2017 (see Fig. 2), when the GDPR had already been enacted. Since then, several research-based PIA methodologies [9,21,50–54,89–91] and standardisation initiatives [18] have been proposed. Nonetheless, advances in developing full-fledged PIA methodologies are still recent, occurring mainly in the past decade.

Considering only the primary research identified in the ScR ($n = 30$), 22 studies (73.3%) published between 2014 and 2023 primarily refer to the GDPR as the motivating legal framework for their research on PIAs. The remaining eight studies were all published before 2017, with three of them referring to the EU Data Protection Directive instead [44,45,49] and five studies concentrated on other privacy regulations [43,61,63, 78,84]. Such findings go to show the expressive impact of the GDPR in the development of PIA methodologies and the existing research on PIAs in practice. On the other hand, this predominance of GDPR-based PIA research may also make it challenging to transfer results to other countries with different privacy laws and PIA requirements. Therefore, non-EU practitioners, researchers, and policymakers should carefully consider existing findings to see if they also apply to their context.

On the other hand, the GDPR has clarified important practical aspects of how PIAs (i.e., DPIAs) should be conducted in an EU context, with such aspects directly connected to our positive and negative subthemes. For instance, issues related to accountability and who is responsible for the implementation of PIAs (Section 4.2.2.N10) were clarified with the entity of a "data controller", bearing the responsibility, and the DPO, obligated to monitor and ensure compliance with the law (Sections 4.2.2.P1 and 4.2.2.P11). The lack of regulatory requirements for PIAs (Section 4.2.2.N11) was also addressed in Article 35 of the GDPR [3], making it mandatory for high-risk systems that process personal data (Section 4.2.2.P1). A PIA must also be prepared *before*

beginning any data processing activity (Section 4.2.2.P2). Moreover, some issues around stakeholder consultation during the PIA process (Section 4.2.2.N7) have also been addressed, highlighting the DPO's role and key stakeholders' engagement in the project (Sections 4.2.2.P4 and 4.2.2.P6).

Furthermore, among the included studies in the ScR, it is clear that [68] remains the most influential piece of work on PIAs in practice. The book was published in the same year that the first proposal of the GDPR was released, compiling knowledge from several privacy practitioners and academics worldwide. To a great extent, the work of Wright and De Hert [68], albeit conducted pre-GDPR, laid the foundation for PIA research in the following years. On the other hand, prominent research has also been published post-GDPR, particularly the works of Ahmadian et al. [50], Horák et al. [48], and Vandercruysse et al. [60], which have been highly cited, presenting important case studies of PIAs in real-world projects, heavily motivated by the challenges of complying with the GDPR legal requirements.

5.2. Overarching research gaps

As evidenced in this ScR, there is an overall lack of literature and research on PIAs in practice, giving rise to different *types of research gaps*, as proposed in [92]. Apart from the limited number of identified studies, many of the publications are book chapters (i.e., $n = 13$, 32.5%), so their findings can be questioned due to the absence of formal scientific peer review. This leaves only 32 peer-reviewed studies (i.e., 17 journal articles, 14 conference papers, and one doctoral thesis). In what follows, future research pathways are introduced according to the four main types of research gaps identified in this ScR, that is, evidence-related, methodological, empirical, and population-related gaps [92].

5.2.1. Evidence gap

There is an evidence gap since many studies yield contradictory results, such as disputing the proven effectiveness of PIA methodologies (Section 4.2.2.N1) [54,55], whether or not PIAs should be mandatory (Section 4.2.2.N6) [75], how to streamline PIA approaches (Section 4.2.2.N1) [75] yet maintaining the assessment comprehensive and rigorous (Section 4.2.2.N2) [43], and the actual feasibility of conducting truly independent PIAs (Section 4.2.2.N14) [6,54]. Finding the balance and achieving consensus on such issues will require further research and discussion among all stakeholders; a one-size-fits-all PIA approach is unlikely.

5.2.2. Methodological gap

This ScR also points to significant methodological gaps, meaning that adequate study designs for the rigorous evaluation of PIA methodologies via empirical inquiry still need to be improved (Section 4.2.2.N1) [54,55]. Furthermore, the critical appraisals for existing studies (Sections 4.3.2 and 4.3.3) point to significant deficiencies in terms of methodological quality, especially concerning the procedures for data collection and analysis. It is also worth noticing that most evidence comes from *Case Study* and *Expert Opinion* publications, which are, regrettably, still at lower levels of evidence strength if compared to other types of study design (e.g., controlled studies, cohort studies, and randomised control trials). The topic of PIAs is currently ripe for further and more sophisticated research designs towards building better evidence from practice.

5.2.3. Empirical gap

Although much research has been published on the broad topic of PIAs and DPIAs, this ScR shows that there is still a lack of empirical studies in real-world practice. This can be considered a major empirical gap concerning the evaluation and practical verification of many other PIA methodologies that have been proposed in recent years. This ScR has identified some prominent studies that help to fill this empirical gap (e.g., [49,52,54,73,84]). However, many other PIA methodologies could still be further evaluated, approaches compared, and studies reproduced, looking to corroborate or add new findings.

This issue concerning the lack of evaluation research on PIAs has also been raised by other researchers (see for instance Friedewald et al. [54]). This lack of evaluation research was also found in the area of privacy engineering in general [10,93]. For this reason, we argue that researchers and practitioners could focus on developing future work on the topic of *Empirical Privacy Engineering*. This includes PIAs/DPIAs and many other theories, methods, techniques, and tools (e.g., privacy threat modelling, privacy risk assessments, requirements engineering for privacy) in the emerging research area of privacy engineering that still need to be rigorously evaluated [93].

5.2.4. Population gap

Another significant challenge refers to the population gap revealed in the included studies, showing that PIA research also suffers from an over-reliance on Western, Educated, Industrialised, Rich, and Democratic (WEIRD) populations [94], mainly from Europe and North America. This ScR has nonetheless identified a minority of studies (*n* = 6, 15%) addressing the practice of PIA in populations from Hong Kong [79], Indonesia [78], Japan [56], India and the Philippines [61], Brazil [66], Syria, Yemen and Iraq [53]. For such reasons, the above-mentioned research gaps have implications for researchers, practitioners, and policymakers tasked with further developing evidence-based PIA practices.

5.2.5. Further systematic reviews

The comprehensive nature of scoping reviews, as explained in Section 3, also enables the identification of potential topics for more focused systemic literature reviews (SLRs). Since this ScR points to a growing maturity of research-based PIA methodologies, one potential topic for a future SLR could be the identification of existing PIA methodologies that have been empirically tested, even if not fully implemented and evaluated in practice. Future SLRs can also focus on how specific stakeholders, such as data subjects, data protection supervisory authorities, or policymakers, perceive and use PIAs. Similarly, other privacy engineering methodologies can be targeted in future systematic reviews, such as model-based approaches for privacy-friendly systems or privacy requirements engineering methods, as identified by Al-Slais [95].

5.3. Considerations for PIA practitioners and policymakers

During this ScR, it was also perceived that some key considerations could be discussed, and recommendations could be drawn to better inform PIA practitioners and policymakers. In what follows, we discuss the risks of distorting PIA attempts and expand on the future requirements (e.g., AI Act) to assess sociotechnical systems from a broader human rights perspective.

5.3.1. The risk of distorting PIAs

A PIA aims at providing an accurate, well-founded, and reliable impact assessment. An erroneous, distorted, or misleading PIA may even create a risk because it should be a reliable basis for taking action, specifically deciding whether the data processing should be conducted as planned and selecting the appropriate technological and organisational measures for sufficiently mitigating the risks (Section 4.2.2.N2) [45,54]. Without a proper basis, the lawfulness of the processing and its compliance with legal provisions may be at stake, there may be undetected risks, and the set of selected measures may not be suitable for proper risk treatment. As a result, the costs may rise if later the processing has to be changed, and additional costs may occur due to fines or financial compensation for data subjects (Section 4.2.2.N3) [8,79].

There are distorted PIAs that are only commissioned work for marketing purposes or even for usage as fig leaf against criticism concerning the processing or the measures taken (Section 4.2.2.N3) [55,63, 86]. But even apart from those PIAs, it is a challenging endeavour to conduct a comprehensive PIA in a neutral way without prejudging the outcome. The team performing the PIA may be professionally blinkered or short-sighted concerning risks due to their experience and their will to reach a positive conclusion instead of identifying risks not yet considered.

Moreover, some methodologies or tools lead to oversimplification or premature results of a PIA. In particular, this is the case if the PIA relies on a *"checklist approach"* [90] (e.g., UK ICO PIA, CNIL PIA), where the PIA team may be tempted to only check off a given list of properties of the IT system without a real understanding of the risks. The same is valid for assessing potential technological and organisational measures [90]. However, it is also worth noting that even thorough PIA methodologies can be misused by practitioners due to their lack of privacy knowledge (Section 4.2.2.N5) [77,83] or due to the perfunctory conduct of PIAs (Section 4.2.2.N3) [55,63].

The PIA should be comprehensible for other parties, including auditors and relevant stakeholders (which may also encompass the public) (Section 4.2.2.P4) [47,54]. Here, it is necessary to decide on the appropriate levels of granularity and complexity [96]. Again, a simple checklist approach would not be fit for this; instead, the performance of a PIA should be considered as an iterative task (Section 4.2.2.P2) [71].

5.3.2. From PIAs to fundamental rights impact assessments

PIAs, and similarly DPIAs, usually focus on the protection of personal data or the privacy of individuals. Thus, the starting point is the (planned) processing of personal data. However, there are further risks to fair design, our society, our planet, and so on. Not all of these additional risks arise from processing personal data, and not all affect individuals, that is, the data subjects in the GDPR terminology. Recognising this limitation, there have been developments towards Human Rights Impact Assessment (HRIA) of digital activities [97] and Fundamental Rights Impact Assessment (FRIA) [98,99].

Recent European legislation, such as the Digital Services Act (DSA, Regulation (EU) 2022/2065) and the upcoming AI Act, demand FRIAs for high-risk data processing contexts. Among others, the risks to be assessed under the DSA regime encompass the dissemination of illegal content, negative effects on civic discourse and the electoral process, public security, and negative effects in relation to gender-based violence, public health protection, the protection of minors, and serious negative consequences to the physical and mental well-being of persons

(Article 34 DSA) [100]. The approach of the AI Act proposal from the European Parliament requires deployers of AI systems to conduct an FRIA of a system in the specific context of use and particularly mentions risks of harm likely to impact marginalised persons or vulnerable groups as well as the reasonably foreseeable adverse impact on the environment [101].

PIAs and DPIAs may be understood as pieces of the bigger picture of an FRIA. The same holds for specific assessments, for instance concerning the impact on civic discourse or the environment. However, it has to be noted that the various impact assessments should not be conducted separately. Instead, a holistic approach is necessary to tackle the interdependencies concerning risks and planned measures to mitigate those risks. Similarly to PIAs, FRIAs would also need to be integrated into the organisational risk management (Section 4.2.2.P8) [74,84].

6. Threats to validity

6.1. Threat I — Limitations of the ScR plan

The first threat relates to the planning of the ScR in terms of identifying the need and justification for this study. Here, we were concerned with identifying existing reviews (systematic and non-systematic) on the topic of PIAs "in the wild". The initial searches did not reveal any review studies on the topic, as described in 3.1.2, pointing to a significant gap in secondary research on PIAs and DPIAs. The planning phase of the ScR is also critical to outline the research questions and provide the basis for an objective investigation of the studies that are being reviewed. If the RQs are not explicitly stated or omit the key topics, the scoping review results can be flawed, overlooking the key information. To mitigate this threat, we outlined three RQs and objectives (Section 3.1.1) that aim to find answers about the frequency, types of research, positive and negative aspects, the strength of primary research, and research gaps. In summary, we seek to minimise any bias or limitations during the planning phase when defining the scope and objectives of this ScR. As a last step in the planning phase, the team finalised and cross-checked the study protocol to minimise the limitations of the ScR plan before proceeding to the subsequent phases.

6.2. Threat II — Credibility of the literature search process

Identifying and selecting the studies reviewed in the ScR are also significant processes to be observed. Selecting studies is a critical step; if any relevant papers are missed, the results of the ScR may be flawed. Therefore, we followed a two-step process (Section 3.2.2), referred to as (i) literature screening and (ii) complete reading of papers. This selection process was carried out independently by two reviewers. We also performed forward and backward snowballing, looking for references to other potentially relevant studies. Also, this ScR restricts the selection of publications to four scientific databases: Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and the OpenGrey database for grey literature. Only these databases were used due to their high relevancy to computer science, privacy, and data protection, as well as to maintain a feasible search space. We essentially used only two broad search terms in this ScR ("privacy impact assessments" and "data protection impact assessments"), maximising the search results; no other constraining terms or filters were necessary since the number of results from this search strategy was still feasible for investigation by the reviewers. This step-wise search process gives us confidence that we minimised limitations related to (i) excluding or overlooking relevant studies or (ii) including irrelevant studies that could impact the results and their reporting in the ScR.

6.3. Threat III — Potential bias in ScR reporting

Some threats should also be considered regarding the potential bias in synthesising the data from the review and documenting the results. This means that if there are some limitations in the data synthesis, they directly impact the results of this ScR. Typical examples of such limitations could be a flawed research taxonomy, incorrect identification of research themes (e.g., positive and negative) and a mismatch of potential research gaps. To minimise the bias in synthesising and reporting the results, we have created a data extraction form that uses well-known classification schemes, such as the ones proposed by Wieringa et al. [37] and Creswell and Creswell [38]. Three researchers independently reviewed this data extraction form while revising the research protocol. While one of the researchers led the data extraction step, two other authors helped by cross-checking the work throughout the process for consistency. Three authors were involved in the thematic analysis of the positive and negative aspects derived from the literature. During the thematic analysis, they actively worked on reviewing the names of codes for consistency and defining themes and sub-themes through a series of meetings. Furthermore, this ScR also offers a complete replication package [36] that conveniently enables other researchers to reproduce or extend this review, as described in Section 3.1.3.

7. Conclusion

Even though PIAs have a long history of developments in the policy arena [2], they must become genuinely evidence-based processes for industry practitioners. Whilst significant contributions have been made in the academic arena concerning PIAs, this ScR shows that the time is ripe for further research since the area is still evolving. In fact, PIAs can be seen as one of the most promising research pathways in the field of Empirical Privacy Engineering, that is, using empirical research methods to study and evaluate engineering approaches for integrating privacy in working systems, taking part in the broad area of empirical software engineering [102,103]. PIAs are a widely known strategy for privacy by design, and many prominent PIA frameworks today still need to be rigorously and independently evaluated. However, developing realistic research designs is a challenge in itself. Furthermore, if the proven effectiveness of PIAs still lacks strong empirical evidence, broader concepts on human rights impact assessments [104] remain arguably even less understood. Nonetheless, based on the existing research, much can be learned, moving towards more evidence-driven PIAs and privacy engineering practices.

CRediT authorship contribution statement

Leonardo Horn Iwaya: Writing – review & editing, Writing – original draft, Visualization, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Ala Sarah Alaqra:** Writing – review & editing, Investigation, Formal analysis, Conceptualization. **Marit Hansen:** Writing – review & editing, Writing – original draft, Formal analysis. **Simone Fischer-Hübner:** Writing – review & editing, Writing – original draft, Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The replication package for this ScR is provided in a public repository [36] and the complete ScR Research Protocol [35].

Appendix A. Critical appraisal checklists

A.1. Critical appraisal of qualitative research

The Checklist for Qualitative Studies from [41] is composed of the following questions (Answers: Yes, No, Cannot tell):

- **Q1.** Did the study address a clearly focused question/issue?
- **Q2.** Is the research method (study design) appropriate for answering the research question?
- **Q3.** Was the context clearly described?
- **Q4.** How was the fieldwork undertaken? Was it described in detail? Are the methods for collecting data clearly described?
- **Q5.** Could the evidence (fieldwork notes, interview transcripts, recordings, documentary analysis, etc.) be inspected independently by others?
- **Q6.** Are the procedures for data analysis reliable and theoretically justified? Are quality control measures used?
- **Q7.** Was the analysis repeated by more than one researcher to ensure reliability?

- **Q8.** Are the results credible, and if so, are they relevant for practice?
- **Q9.** Are the conclusions drawn justified by the results?
- **Q10.** Are the findings of the study transferable to other settings?

A.2. Critical appraisal of quantitative research

The Checklist for Cross-Sectional Studies (Surveys) from [42] is composed of the following questions (Answers: Yes, No, Cannot tell):

- **Q1.** Did the study address a clearly focused question/issue?
- **Q2.** Is the research method (study design) appropriate for answering the research question?
- **Q3.** Is the method of selection of the subjects (employees, teams, divisions, organisations) clearly described?
- **Q4.** Could the way the sample was obtained introduce (selection) bias?
- **Q5.** Was the sample of subjects representative with regard to the population to which the findings will be referred?
- **Q6.** Was the sample size based on pre-study considerations of statistical power?
- **Q7.** Was a satisfactory response rate achieved?
- **Q8.** Are the measurements (questionnaires) likely to be valid and reliable?
- **Q9.** Was the statistical significance assessed?
- **Q10.** Are confidence intervals given for the main results?
- **Q11.** Could there be confounding factors that have not been accounted for?
- **Q12.** Can the results be applied to other organisations?

Appendix B. List of papers in the review

All the studies included in the ScR are listed in Table B.5.

Table B.5
Complete list of papers included in the scoping review. Init Search: studies selected from the initial database searches. FW Snowb (*forward snowballing*): studies that cited the initially selected papers. BW Snowb (*backward snowballing*): studies selected in full-text readings (i.e., in references).

Ref.	Title	Added in
Horák et al. [48]	GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform	Init. Search
Ferra et al. [72]	Challenges in assessing privacy impact: Tales from the front lines	Init. Search
Bräutigam [45]	PIA: Cornerstone of Privacy Compliance in Nokia	Init. Search
Bamberger and Mulligan [63]	PIA Requirements and Privacy Decision-Making in US Government Agencies	Init. Search
Ahmadian et al. [50]	Supporting privacy impact assessment by model-based privacy analysis	Init. Search
Iorio et al. [49]	Privacy impact assessment in the design of transnational public health information systems: The BIRO project	Init. Search
Vandercruysse et al. [60]	A typology of Smart City services: The case of Data Protection Impact Assessment	Init. Search
Iwaya et al. [66]	Mobile health systems for community-based primary care: identifying controls and mitigating privacy threats	Init. Search
Wright et al. [74]	Integrating privacy impact assessment in risk management	Init. Search
Clarke [43]	Privacy impact assessments as a control mechanism for Australian counter-terrorism initiatives	Init. Search
Wright and Wadhwa [75]	Introducing a privacy impact assessment policy in the EU member states	Init. Search
Todde et al. [51]	Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems	Init. Search
Parks et al. [84]	Understanding the drivers and outcomes of healthcare organizational privacy responses	Init. Search
Pribadi and Suryanegara [78]	Regulatory recommendations for IoT smart-health care services by using Privacy Impact Assessment (PIA)	Init. Search
Sharma and Kaushik [61]	Strategy for privacy assurance in offshoring arrangements	Init. Search
Warren and Charlesworth [44]	Privacy impact assessment in the UK	Init. Search
Wright and Hert [62]	Findings and recommendations	Init. Search
Henriksen-Bulmer et al. [52]	DPIA in context: Applying DPIA to assess privacy risks of cyber physical systems	Init. Search
Bayley and Bennett [7]	Privacy impact assessments in Canada	Init. Search
Stoddart [8]	Auditing privacy impact assessments: The Canadian experience	Init. Search

Table B.5 (*continued*).

Ref.	Title	Added in
Bas Seyyar and Geradts [71]	Privacy impact assessment in large-scale digital forensic investigations	Init. Search
Easton [82]	Analysing the Role of Privacy Impact Assessments in Technological Development for Crisis Management	Init. Search
van Puijenbroek and Hoepman [12]	Privacy impact assessment in practice: The results of a descriptive field study in the Netherlands	Init. Search
Waters [79]	Privacy impact assessment - Great potential not often realised	Init. Search
Edwards [6]	Privacy impact assessment in New Zealand - A practitioner's perspective	Init. Search
Kroener et al. [53]	Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems	Init. Search
Shin et al. [56]	Analysis of specific personal information protection assessment in the social security and tax number system of local governments in Japan	Init. Search
Wadhwa [55]	Privacy impact assessment reports: A report card	Init. Search
Stewart [64]	Privacy impact assessment: Optimising the regulator's role	Init. Search
Rehak and Kühne [69]	The Processing goes far beyond "the app"- Privacy issues of decentralized Digital Contact Tracing using the example of the German Corona-Warn-App	Init. Search
Campanile et al. [57]	Evaluating the Impact of Data Anonymization in a Machine Learning Application	Init. Search
Rehak et al. [65]	Analysis and Constructive Criticism of the Official Data Protection Impact Assessment of the German Corona-Warn-App	Init. Search
Friedewald et al. [54]	Data Protection Impact Assessments in Practice: Experiences from Case Studies	Init. Search
Rajamäki [70]	Design Science Research Towards Ethical and Privacy-Friendly Maritime Surveillance ICT Systems	Init. Search
Dashti et al. [77]	Can data subject perception of privacy risks be useful in a data protection impact assessment?	Init. Search
Nas [83]	Data protection impact assessment: Assessing the risks of using Microsoft Office ProPlus	Init. Search
Thoma [46]	How Siemens assesses privacy impacts	Init. Search
Deadman and Chandler [47]	Vodafone's approach to privacy impact assessments	Init. Search
Alaqra et al. [59]	Transparency of Privacy Risks Using PIA Visualizations	Init. Search
Zamorano et al. [67]	Privacy by Design in CBRN Technologies Targeted to Vulnerable Groups: The Case of PROACTIVE	Init. Search
Iwaya et al. [11]	On the privacy of mental health apps: An empirical investigation and its implications for app development	Init. Search
Schneider et al. [23]	Persona-oriented Data Protection Impact Assessment for Small Businesses	Init. Search
Alaqra et al. [58]	Machine learning–based analysis of encrypted medical data in the cloud: Qualitative study of expert stakeholders' perspectives	BW Snowb.
Vandercruysse et al. [73]	The DPIA: Clashing Stakeholder Interests in the Smart City?	FW Snowb.
McKee [9]	Privacy Assessment Breakthrough: A Design Science Approach to Creating a Unified Methodology	FW Snowb.

References

[1] Wright D. The state of the art in privacy impact assessment. Comput Law Secur Rev 2012;28(1):54–61.

[2] Clarke R. Privacy impact assessment: Its origins and development. Comput Law Secur Rev 2009;25(2):123–35. http://dx.doi.org/10.1016/j.clsr.2009.02.002, URL https://www.sciencedirect.com/science/article/pii/S0267364909000302.

[3] Commission E. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J Eur Union 2016;119(April):1–88.

[4] Commission E. Charter of fundamental rights of the European union (2012/c 326/02). (October). 2012, URL https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT,

[5] Hallinan D, Martin N. Fundamental rights, the normative keystone of DPIA. Eur Data Prot Law Rev 2020;6:178–93. http://dx.doi.org/10.21552/edpl/2020/2/6.

[6] Edwards J. Privacy impact assessment in New Zealand – A practitioner's perspective. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 187–204.

[7] Bayley RM, Bennett CJ. Privacy impact assessments in Canada. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 161–85.

[8] Stoddart J. Auditing privacy impact assessments: The Canadian experience. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 419–36.

[9] McKee L. Privacy assessment breakthrough: A design science approach to creating a unified methodology (Ph.D. thesis), Dakota State University; 2022, https://scholar.dsu.edu/theses/382.

[10] Iwaya LH, Babar MA, Rashid A. Privacy engineering in the wild: Understanding the practitioners' mindset, organisational aspects, and current practices.

IEEE Trans Softw Eng 2023;49(9):1–26. http://dx.doi.org/10.1109/TSE.2023.3290237.

[11] Iwaya LH, Babar MA, Rashid A, Wijayarathna C. On the privacy of mental health apps: An empirical investigation and its implications for app development. Empir Softw Eng 2023;28(1):2. http://dx.doi.org/10.1007/s10664-022-10236-0.

[12] van Puijenbroek J, Hoepman J-H. Privacy impact assessments in practice: Outcome of a descriptive field research in the Netherlands. In: In alamo, JM del (ed.), IWPE 2017: international workshop on privacy engineering: proceedings of the 3rd international workshop on privacy engineering, co-located with 38th IEEE symposium on security and privacy (s&p 2017). San Jose (CA), USA: CEUR Workshop Proceedings; 2017, p. 1–8.

[13] OPC. Privacy impact assessment handbook. 2007, URL https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-Impact-Assessment-Handbook-June2007.pdf. Office of the Privacy Commissioner.

[14] Oetzel MC, Spiekermann S, Grüning I, Kelter H, Mull S. Privacy impact assessment guideline. 2011, URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfasssung.pdf?__blob=publicationFile&v=1. Bundesamt für Sicherheit in der Informationstechnik.

[15] Oetzel MC, Spiekermann S, Grüning I, Kelter H, Mull S. Privacy impact assessment guideline for RFID applications. 2011, URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1. Bundesamt für Sicherheit in der Informationstechnik.

[16] CNIL. Privacy impact assessment (PIA) methodology (how to carry out a PIA). 2015, URL https://www.cnil.fr/sites/cnil/files/typo/document/CNIL-PIA-1-Methodology.pdf. Commission nationale de l'informatique et des libertés.

[17] OAIC. Guide to undertaking privacy impact assessments. 2020, URL https://www.oaic.gov.au/_data/assets/pdf_file/0013/2074/guide-to-undertaking-privacy-impact-assessments.pdf. Office of the Australian Information Commissioner.

[18] ISO/IEC 29134:2023. Information technology - Security techniques - Guidelines for privacy impact assessment. Standard, Geneva, CH: International Organization for Standardization; 2023.

[19] WP29. Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679. 2017, URL https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711. EU Commission.

[20] SGTF. Data protection impact assessment for smart grid and smart metering environment. 2018, URL https://energy.ec.europa.eu/system/files/2018-09/dpia_for_publication_2018_0.pdf. Smart Grids Task Force (SGTF) - Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment.

[21] Reuben J, Martucci LA, Fischer-Hübner S, Packer HS, Hedbom H, Moreau L. Privacy impact assessment template for provenance. In: 2016 11th international conference on availability, reliability and security. ARES, Salzburg, Austria: IEEE; 2016, p. 653–60.

[22] Mantovani E, Antokol J, Hoekstra M, Nouwt S, Schutte N, Zilgalvis P, Castro Gómez-Valadés J-P, Prettner C. Towards a code of conduct on privacy for mhealth to foster trust amongst users of mobile health applications. Data Prot Priv: Vis Infrastruct 2017;81–106.

[23] Schneider B, Asprion PM, Misyura I, Jonkers N, Zaugg E. Persona-oriented data protection impact assessment for small businesses. EPiC Ser Comput 2023;93:152–63.

[24] ICO. Accountability and governance data protection impact assessments (DPIAs). 2018, URL https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias-1-0.pdf. Information Commissioner's Office.

[25] Oetzel MC, Spiekermann S. A systematic methodology for privacy impact assessments: A design science approach. Eur J Inf Syst 2014;23(2):126–50, arXiv:https://doi.org/10.1057/ejis.2013.18. URL https://doi.org/10.1057/ejis.2013.18.

[26] Vemou K, Karyda M. An evaluation framework for privacy impact assessment methods. In: Mediterranean conference on information systems. MCIS 2018, AIS eLibrary; 2018, p. 5.

[27] Vemou K, Karyda M. Evaluating privacy impact assessment methods: Guidelines and best practice. Inf Comput Secur 2019;28(1):35–53.

[28] Bisztray T, Gruschka N. Privacy impact assessment: comparing methodologies with a focus on practicality. In: Nordic conference on secure IT systems. Springer; 2019, p. 3–19.

[29] Wairimu S, Iwaya LH, Fritsch L, Lindskog S. On the evaluation of privacy impact assessment and privacy risk assessment methodologies: A systematic literature review. IEEE Access 2024;12:19625–50. http://dx.doi.org/10.1109/ACCESS.2024.3360864.

[30] Tricco AC, Lillie E, Zarin W, O'Brien KK, Colquhoun H, Levac D, Moher D, Peters MD, Horsley T, Weeks L, et al. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. Ann Internal Med 2018;169(7):467–73.

[31] Moher D, Shamseer L, Clarke M, Ghersi D, Liberati A, Petticrew M, Shekelle P, Stewart LA. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. Syst Rev 2015;4(1):1–9.

[32] Arksey H, O'Malley L. Scoping studies: towards a methodological framework. Int J Soc Res Methodol 2005;8(1):19–32.

[33] Tricco AC, Lillie E, Zarin W, O'Brien K, Colquhoun H, Kastner M, Levac D, Ng C, Sharpe JP, Wilson K, et al. A scoping review on the conduct and reporting of scoping reviews. BMC Med Res Methodol 2016;16(1):1–10.

[34] Munn Z, Peters MD, Stern C, Tufanaru C, McArthur A, Aromataris E. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Methodol 2018;18:1–7.

[35] Iwaya LH. Privacy impact assessments in the wild: Scoping review protocol. 2023, URL https://github.com/lhiwaya/ScR-PIAs-Wild/blob/main/Privacy_Impact_Assessments_in_the_Wild__ScR_Protocol_v1.1.pdf. Privacy and Security Research Group.

[36] Iwaya LH. PIAs in the wild scoping review - replication package. 2024, URL https://github.com/lhiwaya/ScR-PIAs-Wild. Privacy and Security Research Group.

[37] Wieringa R, Maiden N, Mead N, Rolland C. Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requir Eng 2006;11(1):102–7.

[38] Creswell JW, Creswell JD. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. United States: Sage publications; 2017.

[39] Shaw M. Writing good software engineering research papers. In: 25th international conference on software engineering, 2003. proceedings.. Portland, OR, USA: IEEE; 2003, p. 726–36.

[40] Braun V, Clarke V. Using thematic analysis in psychology. Qual Res Psychol 2006;3(2):77–101.

[41] CEBMa. Critical appraisal checklist for a qualitative study. 2014, URL https://cebma.org/wp-content/uploads/Critical-Appraisal-Questions-for-a-Qualitative-Study-July-2014-1.pdf, Center for Evidence-Based Management, Amsterdam, The Netherlands.

[42] CEBMa. Critical appraisal checklist for cross-sectional study. 2014, URL https://cebma.org/wp-content/uploads/Critical-Appraisal-Questions-for-a-Cross-Sectional-Study-July-2014-1.pdf, Center for Evidence-Based Management, Amsterdam, The Netherlands.

[43] Clarke R. Privacy impact assessments as a control mechanism for Australian counter-terrorism initiatives. Comput Law Secur Rev 2016;32(3):403–18. http://dx.doi.org/10.1016/j.clsr.2016.01.009, URL https://www.sciencedirect.com/science/article/pii/S0267364916300231.

[44] Warren A, Charlesworth A. Privacy impact assessment in the UK. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 205–24.

[45] Bräutigam T. PIA: Cornerstone of privacy compliance in nokia. In: Privacy impact assessment. Dordrecht: Springer Netherlands; 2012, p. 253–74, URL https://doi.org/10.1007/978-94-007-2543-0_11.

[46] Thoma F. How Siemens assesses privacy impacts. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 275–84.

[47] Deadman S, Chandler A. Vodafone's approach to privacy impact assessments. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 285–304.

[48] Horák M, Stupka V, Husák M. GDPR compliance in cybersecurity software: A case study of DPIA in information sharing platform. In: Proceedings of the 14th international conference on availability, reliability and security. ARES '19, New York, NY, USA: Association for Computing Machinery; 2019, URL https://doi.org/10.1145/3339252.3340516.

[49] Iorio CTD, Carinci F, Azzopardi J, Baglioni V, Beck P, Cunningham S, Evripidou A, Leese G, Loevaas KF, Olympios G, Federici MO, Pruna S, Palladino P, Skeie S, Taverner P, Traynor V, Benedetti MM. Privacy impact assessment in the design of transnational public health information systems: the BIRO project. J Med Ethics 2009;35(12):753–61. http://dx.doi.org/10.1136/jme.2009.029918, arXiv:https://jme.bmj.com/content/35/12/753.full.pdf. URL https://jme.bmj.com/content/35/12/753.

[50] Ahmadian AS, 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. SAC '18, New York, NY, USA: Association for Computing Machinery; 2018, p. 1467–74, URL https://doi.org/10.1145/3167132.3167288.

[51] Todde M, Beltrame M, Marceglia S, Spagno C. Methodology and workflow to perform the data protection impact assessment in healthcare information systems. Inform Med Unlocked 2020;19:100361. http://dx.doi.org/10.1016/j.imu.2020.100361, URL https://www.sciencedirect.com/science/article/pii/S2352914820301477.

[52] Henriksen-Bulmer J, Faily S, Jeary S. DPIA in context: Applying DPIA to assess privacy risks of cyber physical systems. Future Internet 2020;12(5):1–23. http://dx.doi.org/10.3390/fi12050093, URL https://www.mdpi.com/1999-5903/12/5/93.

[53] Kroener I, Barnard-Wills D, Muraszkiewicz J. Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems. Ethics Inf Technol 2021;23:7–18.

[54] Friedewald M, Schiering I, Martin N, Hallinan D. Data Protection Impact Assessments in Practice: Experiences from Case Studies. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 13106 LNCS, 2022, p. 424–43. http://dx.doi.org/10.1007/978-3-030-95484-0_25.

[55] Wadhwa K. Privacy impact assessment reports: A report card. Info 2012;14(3):35–47.

[56] Shin S, Seto Y, Sasaki M, Sakamoto K. Analysis of specific personal information protection assessment in the social security and tax number system of local governments in Japan. In: Saeed K, Homenda W, Chaki R, editors. Computer information systems and industrial management. Cham: Springer International Publishing; 2017, p. 685–96.

[57] Campanile L, Forgione F, Mastroianni M, Palmiero G, Sanghez C. Evaluating the impact of data anonymization in a machine learning application. In: Gervasi O, Murgante B, Misra S, Rocha AMAC, Garau C, editors. Computational science and its applications – ICCSA 2022 workshops. Cham: Springer International Publishing; 2022, p. 389–400.

[58] Alaqra AS, Kane B, Fischer-Hübner S. Machine learning–based analysis of encrypted medical data in the cloud: Qualitative study of expert stakeholders' perspectives. JMIR Hum Factors 2021;8(3):e21810.

[59] Alaqra AS, Fischer-Hübner S, Karegar F. Transparency of privacy risks using PIA visualizations. In: Moallem A, editor. HCI for cybersecurity, privacy and trust. Cham: Springer Nature Switzerland; 2023, p. 3–17.

[60] Vandercruysse L, Buts C, Dooms M. A typology of smart city services: The case of data protection impact assessment. Cities 2020;104:102731. http://dx.doi.org/10.1016/j.cities.2020.102731, URL https://www.sciencedirect.com/science/article/pii/S026427511931203X.

[61] Sharma C, Kaushik A. Strategy for privacy assurance in offshoring arrangements. J Glob Oper Strateg Sour 2017;10(2):232–54.

[62] Wright D, Hert PD. Findings and recommendations. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 445–81.

[63] Bamberger KA, Mulligan DK. PIA requirements and privacy decision-making in US government agencies. In: Privacy impact assessment. Dordrecht: Springer Netherlands; 2012, p. 225–50, URL https://doi.org/10.1007/978-94-007-2543-0_10.

[64] Stewart B. Privacy impact assessment: Optimising the regulator's role. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 437–44.

[65] Rehak R, Kühne CR, Bock K. Analysis and constructive criticism of the official data protection impact assessment of the german corona-warn-app. In: Gryszczyńska A, Polański P, Gruschka N, Rannenberg K, Adamczyk M, editors. Privacy technologies and policy. Cham: Springer International Publishing; 2022, p. 119–34.

[66] Iwaya LH, Fischer-Hübner S, Å hlfeldt R-M, Martucci LA. Mobile health systems for community-based primary care: Identifying controls and mitigating privacy threats. JMIR mHealth uHealth 2019;7(3):e11642.

[67] Zamorano MM, Newton N, Bertelli V, Petersen L. Privacy by design in CBRN technologies targeted to vulnerable groups: The case of PROACTIVE. In: International conference on information technology in disaster risk reduction. Springer; 2022, p. 244–58.

[68] Wright D, De Hert P. Privacy impact assessment. Vol. 6, Dordrecht: Springer; 2012.

[69] Rehak R, Kühne CR. The processing goes far beyond "the app" – privacy issues of decentralized digital contact tracing using the example of the german corona-warn-app. In: 2022 6th international conference on cryptography, security and privacy. CSP, Tianjin, China: IEEE; 2022, p. 16–20. http://dx.doi.org/10.1109/CSP55486.2022.00011.

[70] Rajamäki J. Design science research towards ethical and privacy-friendly maritime surveillance ICT systems. In: Digital transformation, cyber security and resilience of modern societies. Cham: Springer International Publishing; 2021, p. 95–115, URL https://doi.org/10.1007/978-3-030-65722-2_7.

[71] Bas Seyyar M, Geradts Z. Privacy impact assessment in large-scale digital forensic investigations. Forensic Sci Int: Digit Invest 2020;33:200906. http://dx.doi.org/10.1016/j.fsidi.2020.200906, URL https://www.sciencedirect.com/science/article/pii/S2666281720300263.

[72] Ferra F, Wagner I, Boiten E, Hadlington L, Psychoula I, Snape R. Challenges in assessing privacy impact: Tales from the front lines. Secur Priv 2020;3(2):e101.

[73] Vandercruysse L, Dooms M, Buts C. The DPIA: Clashing stakeholder interests in the smart city? In: Data protection and privacy: enforcing rights in a changing world. first ed.. Vol. 14, London: Bloomsbury; 2021, p. 245–84.

[74] Wright D, Wadhwa K, Lagazio M, Raab C, Charikane E. Integrating privacy impact assessment in risk management. Int Data Priv Law 2014;4(2):155–70.

[75] Wright D, Wadhwa K. Introducing a privacy impact assessment policy in the EU member states. Int Data Priv Law 2013;3(1):13–28.

[76] Pulls T, Fritsch L, Iwaya LH, Karegar F, Palomares A, Baún JCP. D3.2 - risk management artefacts for increased transparency. 2019, URL https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c6481c64&appId=PPGMS. EU Commission.

[77] Dashti S, Santana de Oliveria A, Kaplan C, Dalcastagne M, Ranise S. Can data subject perception of privacy risks be useful in a data protection impact assessment? In: Proceedings of the 18th international conference on security and cryptography - SECRYPt,. Setubal, Portugal: SciTePress. INSTICC; 2021, p. 827–32. http://dx.doi.org/10.5220/0010602608270832.

[78] Pribadi IL, Suryanegara M. Regulatory recommendations for IoT smart-health care services by using privacy impact assessment (PIA). In: 2017 15th international conference on quality in research (qiR): international symposium on electrical and computer engineering. Nusa Dua, Bali, Indonesia: IEEE; 2017, p. 491–6.

[79] Waters N. Privacy impact assessment – great potential not often realised. In: Privacy impact assessment. Dordrecht: Springer; 2012, p. 149–60.

[80] CNIL. Privacy impact assessment (PIA) templates. 2018, URL https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-2-en-templates.pdf. Commission nationale de l'informatique et des libertés.

[81] CNIL. Privacy impact assessment (PIA) knowledge bases. 2018, URL https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf. Commission nationale de l'informatique et des libertés.

[82] Easton C. Analysing the role of privacy impact assessments in technological development for crisis management. J Contin Crisis Manage 2017;25(1):7–14. http://dx.doi.org/10.1111/1468-5973.12140, URL https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-5973.12140.

[83] Nas S. Data protection impact assessment: Assessing the risks of using microsoft office ProPlus. Eur. Data Prot. L. Rev. 2019;5:107.

[84] Parks R, Chu CH, Xu H, Adams L. Understanding the drivers and outcomes of healthcare organizational privacy responses. In: 32nd international conference on information system 2011, ICIS 2011. Shanghai: AIS eLibrary; 2011, p. 245–64.

[85] Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, Stoddart K. A review of cyber security risk assessment methods for SCADA systems. Comput Secur 2016;56:1–27. http://dx.doi.org/10.1016/j.cose.2015.09.009.

[86] Warren A, Bayley R, Bennett C, Charlesworth A, Clarke R, Oppenheim C. Privacy impact assessments: International experience as a basis for UK guidance. Comput Law Secur Rev 2008;24(3):233–42.

[87] Clarke R, et al. An evaluation of privacy impact assessment guidance documents. Int Data Priv Law 2011;1(2):111–20.

[88] Commission E. Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2012, URL https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011,

[89] De SJ, Le Métayer D. PRIAM: a privacy risk analysis methodology. In: Data privacy management and security assurance: 11th international workshop, DPM 2016 and 5th international workshop, QASA 2016, heraklion, crete, Greece, September 26-27, 2016, proceedings 11. Cham: Springer; 2016, p. 221–9.

[90] Bieker F, Friedewald M, Hansen M, Obersteller H, Rost M. A process for data protection impact assessment under the European general data protection regulation. In: Privacy technologies and policy: 4th annual privacy forum, APF 2016, frankfurt/main, Germany, September 7-8, 2016, proceedings 4. Cham: Springer; 2016, p. 21–37.

[91] Timón López C, Alamillo Domingo I, Valero Torrijos J. Approaching the data protection impact assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. a special reference to identity management systems. In: Proceedings of the 16th international conference on availability, reliability and security. Vienna, Austria: Association for Computing Machinery; 2021, p. 1–9.

[92] Miles DA. A taxonomy of research gaps: Identifying and defining the seven research gaps, doctoral student workshop: finding research gaps-research methods and strategies, dallas, texas. 2017, p. 15, URL https://www.researchgate.net/publication/319244623.

[93] Gurses S, del Alamo JM. Privacy engineering: Shaping an emerging field of research and practice. IEEE Secur Priv 2016;14(02):40–6. http://dx.doi.org/10.1109/MSP.2016.37.

[94] Henrich J, Heine SJ, Norenzayan A. Most people are not WEIRD. Nature 2010;466(7302):29.

[95] Al-Slais Y. Privacy engineering methodologies: A survey. In: 2020 international conference on innovation and intelligence for informatics, computing and technologies. 3ICT, 2020, p. 1–6. http://dx.doi.org/10.1109/3ICT51146.2020.9311949.

[96] Martin N, Friedewald M, Schiering I, Mester BA, Hallinan D, Jensen M. The data protection impact assessment according to article 35 GDPR - A practitioner's manual. Technical Report, Fraunhofer; 2020.

[97] DIHR. Guidance on human rights impact assessment of digital activities. 2020, URL https://www.humanrights.dk/publications/human-rights-impact-assessment-digital-activities. The Danish Institute for Human Rights.

[98] Janssen H, Seng Ah Lee M, Singh J. Practical fundamental rights impact assessments. Int J Law Inf Technol 2022;30(2):200–32, URL https://doi.org/10.1093/ijlit/eaac018.

[99] BZK. Impact assessment fundamental rights and algorithms. 2022, URL https://www.government.nl/documents/reports/2022/03/31/impact-assessment-fundamental-rights-and-algorithms. Dutch Ministry of the Interior and Kingdom Relations.

[100] Mantelero A. Fundamental rights impact assessment in the DSA. In: Putting the DSA into practice. Berlin: Verfassungsblog; 2023, p. 107–19, URL https://doi.org/10.17176/20230208-093135-0.

[101] Parliament E. Artificial Intelligence Act Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). 2023, URL https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf. EU Parliament.

[102] Guéhéneuc Y-G, Khomh F. Empirical software engineering. In: Handbook of software engineering. Cham: Springer; 2019, p. 285–320.

[103] Fernández DM, Passoth J-H. Empirical software engineering: from discipline to interdiscipline. J Syst Softw 2019;148:170–9.

[104] De Beco G. Human rights impact assessments. Neth Q Hum Rights 2009;27(2):139–66.