information

MDPI

Article

Addressing Data Protection Impact Assessment (DPIA) Implementation Challenges in AI-Driven Digitalisation: A Systematic Review and PDCA-Based Governance Framework

Bilgin Metin [1], Nazlı Elif Yey [1] and Martin Wynn [2,*]

[1] Management Information Systems Department, Bogazici University, Istanbul 34342, Turkey; bilgin.metin@bogazici.edu.tr (B.M.); nazli.yey.2024@alumni.boun.edu.tr (N.E.Y.)
[2] School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL50 2RH, UK
* Correspondence: mwynn@glos.ac.uk

Abstract

AI-driven digitalisation transforms how organisations process personal data and introduces risks that traditional Data Protection Impact Assessment (DPIA) frameworks cannot adequately address. Automated decision-making and large-scale processing in AI, IoT, big data analytics, and blockchain environments create privacy concerns beyond the scope of existing DPIA methodologies. The EU AI Act extends this scope through the Fundamental Rights Impact Assessment (FRIA) under Article 27, which links data protection obligations to broader fundamental rights governance. This study addresses these gaps through a two-phase research design. Phase 1 conducts a systematic literature review of 25 studies and applies framework analysis to identify DPIA implementation challenges across four categories: legal and regulatory, risk assessment, scope, and complexity. AI-specific challenges appear across all four categories. Phase 2 develops a governance framework built on the Plan-Do-Check-Act (PDCA) cycle and organised through a four-level hierarchy of Lifecycle Phase, Risk Management Domain, Control Objective, and Operational Activity. The framework translates relevant requirements of ISO 31000:2018, ISO/IEC 27701:2025, and ISO/IEC 29134:2023 into traceable activities and encompasses algorithmic fairness and socio-ethical impacts. The actionable DPIA framework supports compliance with the GDPR, the EU AI Act and the three ISO standards and will be of interest to company practitioners and other researchers investigating the theoretical and practice-based aspects of digitalisation and data privacy.

Keywords: general data protection regulation; GDPR; data protection impact assessment; DPIA; privacy impact assessment; PIA; data protection; technological advancements; personal data processing; AI; artificial intelligence; AI-driven digitalisation

Academic Editor: Eric Pardede

Received: 29 May 2026
Revised: 27 June 2026
Accepted: 3 July 2026
Published: 13 July 2026

1. Introduction

In an age of rapid artificial intelligence (AI)-driven technological advancements, the challenges of Data Protection Impact Assessment (DPIA) have become increasingly complex and significant. The rapid growth of digital innovation in organisations has introduced new dimensions in the management and protection of sensitive information, whilst digital transformation has led to changes in company structures and triggered new organisational forms [1,2]. At the same time, however, there are some growing concerns around the secure and lawful processing of personal data under current legal frameworks [3]: while digital technologies and services generally benefit businesses and consumers, they also

pose serious privacy risks [4,5]. As organisations strive to leverage the benefits of AI-driven digitalisation for innovation and growth, they are also faced with the daunting task of ensuring the privacy and security of personal data.

Article 35 of the Regulation (EU) 2016/679, referred to as General Data Protection Regulation (GDPR) [6], requires a DPIA where the processing of personal data may pose high risks to data protection and privacy and may adversely affect the rights and freedoms of individuals. The DPIA is a systematic and comprehensive analysis by data controllers. It enables them to mitigate potential compliance issues before embarking on a data processing activity that, by its nature, scope, context and purposes, may pose high risks to the rights and freedoms of individuals and may be of critical importance for organisations. This is especially the case with large-scale data processing activities, the processing of special categories of personal data, the systematic and comprehensive assessment of personal aspects relating to natural persons based on automated data processing, including profiling, or where a new technology is used. DPIA obligations also apply when personal data is transferred to or processed by third-party processors or sub-processors, including cloud service providers. Under GDPR Article 28, data controllers must ensure that all processors implement appropriate technical and organisational security measures, and the DPIA must cover the full processing chain. In cloud environments, this requires particular attention to data sovereignty, encryption of data in transit and at rest, access control governance, and the auditability of provider-level security controls. Organisations should take concrete steps to comply with the legal obligations introduced by the concept of "privacy by design and by default", which is based on the understanding that it is preferable to build privacy features into a product or service from the outset, rather than in the later stages of product or services design [3].

The regulatory landscape continues to evolve in response to these technological developments. The recently adopted Regulation (EU) 2024/1689, also referred to as the European Union Artificial Intelligence (AI) Act [7] broadens the concept of "high risk" to include certain artificial intelligence (AI) applications whose outcomes could have a significant impact on individuals' rights and opportunities [8]. The AI Act [7] defines "high-risk AI systems" through a risk-based classification set out in Article 6 and Annex III. This covers sensitive use cases such as biometric identification, access to essential services, employment and worker management, education, and specific law enforcement and migration contexts. In these areas, AI systems are considered high risk because their decisions can directly affect a person's legal position, social prospects, or access to essential services. Accordingly, the AI Act [7] requires additional safeguards, including dedicated assessments of the impact on fundamental rights, to complement the DPIA required under Article 35 of the GDPR when high-risk AI systems are deployed. Article 27 of the AI Act [7] introduces the obligation to conduct a Fundamental Rights Impact Assessment (FRIA). In this regard, GDPR-based DPIAs and AI Act-based FRIAs may substantially overlap where high-risk AI systems process personal data [9]. This extends the scope of the DPIA beyond data protection risks, capturing broader risks to fundamental rights such as fairness, non-discrimination and equal treatment. This approach reflects a broader shift in impact assessment practices, whereby the DPIA evolves from a standalone compliance tool into an integrated risk governance mechanism that considers the data protection and broader socio-technical implications of digital technology deployment.

This evolution of impact assessment practices, driven by both technological change and regulatory developments such as the GDPR [6] and the AI Act [7], builds on earlier approaches to privacy risk assessment. Although the DPIA concept was introduced with the GDPR, it built upon the Privacy Impact Assessment (PIA) [10], which dates from the mid-1990s, and which aimed to help organisations determine the most effective way to comply

with their data protection obligations and meet individuals' privacy expectations [11]. It purported that organisations should build data protection into the lifecycle of data processing activities by being aware of any potential negative impact that personal data processing activities may have on individuals' rights and freedoms from the outset and in all aspects. Definitions of DPIA and PIA by various data protection entities are shown in Table A1 in Appendix A.

The Article 29 Working Party [12] defines DPIA as a process designed to identify processing, to assess its necessity and proportionality, and to help manage it by assessing the risks to the rights and freedoms of natural persons arising from the processing of personal data and identifying measures to address them. Under the GDPR, the data controller is obliged to carry out a DPIA before processing activities which, due to their nature, scope or purposes, pose specific risks to the rights and freedoms of the data subject. This is of particular relevance when personal aspects of the data subject are systematically and extensively assessed for automated decisions, if special categories of personal data are processed on a large scale, or if a publicly accessible area is systematically monitored on a large scale. However, there is currently very little known about how to conduct such a DPIA in the context of digital technology deployment, for example as regards big data analytics [3]. Recent studies further suggest that DPIA implementation practices remain heterogeneous and insufficiently standardised, particularly regarding operational implementation processes and methodological guidance [13]. This article explores the key challenges that organisations encounter in conducting DPIAs in the era of digital innovation.

Despite significant academic interest in the implementation of DPIAs and the challenges organisations face as technology evolves, most research so far has concentrated on privacy and data protection issues within industry and public administration. Through a critical analysis of the literature, this paper addresses this gap by examining the challenges of digitalisation and open digital innovation for organisations, and by shedding light on the complexities and nuances of DPIA in the context of digitalisation. The article also draws upon the governance model adopted in ISO/IEC 27701 [14], which aligns privacy management with other management system standards by embedding iterative monitoring, performance evaluation, and adaptive review mechanisms, epitomised by the Plan–Do–Check–Act (PDCA) cycle. In this context, the article addresses the following research questions (RQs):

RQ1. *What challenges were encountered in implementing the DPIA, particularly in the area of technology-based data processing?*

RQ2. *Can a framework be developed to address the DPIA implementation challenges for digital technologies?*

The contribution of this study is conceptual and normative rather than empirical. It synthesises a fragmented body of literature into a structured challenge taxonomy and proposes a governance framework that translates established standards into traceable operational activities. The framework is offered as a theoretically grounded and standards-aligned proposal to guide DPIA practice; it is not an empirically tested implementation model, and its operational validation in organisational settings remains an objective for future research.

Following this brief introduction, Section 2 details the study's methodology, including the search strategy, inclusion and exclusion criteria, data extraction procedures, and quality assessment. In Section 3, an overview of the findings is first provided, and then RQ1 is addressed and a categorization of DPIA challenges, derived from the extant literature, is put forward. This acts as the basis for addressing RQ2 through the development of a PDCA-based framework, which directly addresses the challenges identified, encompassing technical, legal, and socio-ethical dimensions, to underpin a thorough and integrated

risk assessment approach. In Section 4, some emergent issues of relevance are discussed. Finally, Section 5 provides a conclusion, summarising the contribution of the research, its limitations and possible future avenues of research in this field of study.

2. Research Methods

The research adopted an interpretivist philosophy, which allowed the capture of context specific realities regarding DPIA use in practice [15]. Concepts and findings were developed inductively in line with Thomas's [16] approach to qualitative data analysis. Saunders et al.'s [17] typology of research methods was also used, combining exploratory aims (to assess current DPIA deployment) with descriptive profiling (of current digital technology contexts). The research was conducted in two phases (Figure 1).

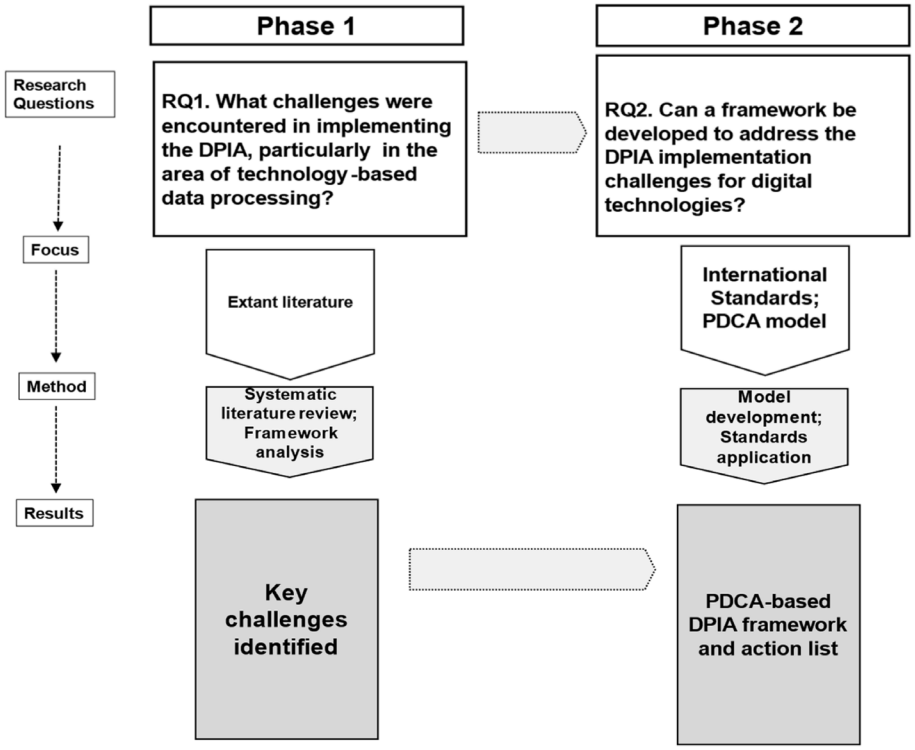

Figure 1. The two-phase research process.

Phase 1 involved a systematic literature review (SLR) which was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines [18]. The PRISMA Flow Diagram is shown in Figure 2. The search included reputable academic databases (Scopus and Web of Science) providing access to peer-reviewed journals, conference proceedings and reports. The search for relevant articles was conducted by examining the title, abstract, and keyword sections of the Scopus and Web of Science databases. The search strategy included various combinations of keywords related to the challenges organisations face when implementing DPIA in the context of technological developments, utilising Boolean operators ('AND' and 'OR') to combine the search terms. The search terms used for the literature review were as follows:

("data protection impact assessment" OR "DPIA" OR "privacy impact assessment" OR "pia")

AND

("General Data Protection Regulation" OR "GDPR")

AND

("implementation" OR "challenges").

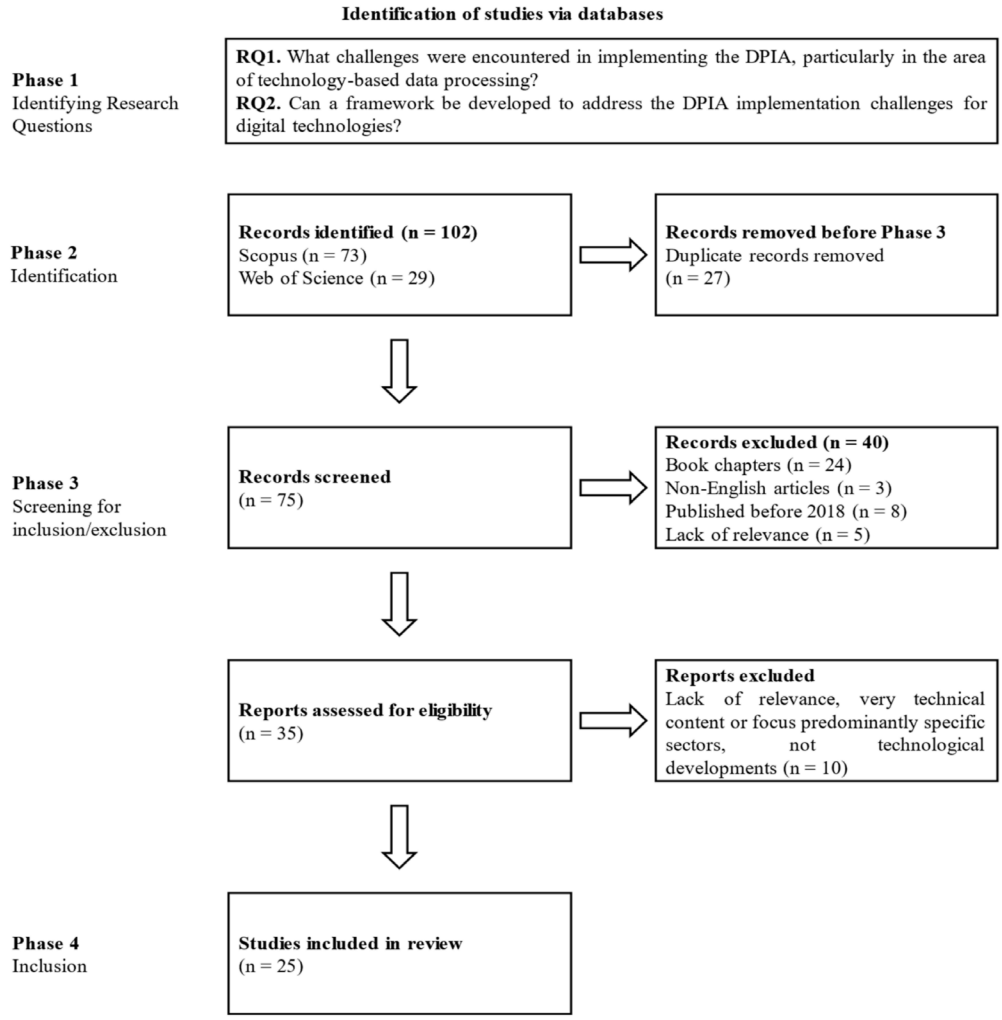

Figure 2. Systematic Literature Review: PRISMA Flow Diagram.

To increase the accuracy of the search, it was later narrowed down to specific types of documents, years, and languages. The initial search yielded 102 documents, which were then screened for eligibility for the study. After eliminating duplicates, 75 documents were further screened using inclusion/exclusion methods (Table 1). The initial sample of potentially relevant studies was analysed and general inclusion and exclusion criteria were applied to refine the selection. Articles published in peer-reviewed journals and conference proceedings were included but studies from books and book series were excluded. In addition, non-English documents were excluded to ensure a clear understanding of the content of each eligible article. Furthermore, the focus was on articles published from 2018 onwards, when the GDPR came into full effect. Subsequently, the titles and abstracts of all remaining articles were manually scanned to assess their relevance to the research topic of challenges in implementing DPIA with technological developments. All irrelevant articles were discarded, including those focusing on the impact of DPIA implementation in non-EU countries.

After the initial screening process, 35 eligible studies were identified for further review. These articles were thoroughly reviewed to assess their relevance to the purpose of this review. As part of this assessment, 10 studies were excluded for various reasons. These reasons included lack of relevance, highly technical content, and a focus on challenges specific to building only GDPR-compliant data architecture. In addition, specific/narrow sectors which were not focused on technological developments such as drones and smart city services, including smart city data ecosystem studies. Here, the scope is often too

narrow and context-dependent, addressing DPIA challenges unique to heterogeneous urban data flows and multi-stakeholder environments but not offering a generalisable DPIA methodology beyond the smart city data ecosystem context [19].

Table 1. Inclusion and exclusion criteria.

Criteria	Principle
Inclusion	- English language articles - Articles published between 2018 and 2026 - Publications in peer-reviewed journals and conference proceedings - Relevance of title and abstract to DPIA implementation challenges - Studies focusing on the impact of DPIA in the EU
Exclusion	- Non-English language articles - Articles published before 2018 - Studies published in books and book series - Studies that do not specifically focus on DPIA implementation challenges - Studies focusing on the impact of DPIA outside the EU

The exclusion principle applied to sectoral studies took into account their transferability: studies were excluded when their identified DPIA challenges were unique to a specific sectoral context and could not be abstracted into generalizable implementation barriers. Studies addressing DPIA challenges in healthcare ICT infrastructures, AI decision-making systems, and blockchain-based IoT environments were retained because the technological challenges they address—automated processing, complex multi-stakeholder data flows, and the integration of security and privacy assessment—are representative of the broader AI-driven digitalisation context the proposed framework addresses. By contrast, studies focusing on DPIA challenges unique to heterogeneous urban data flows in smart city ecosystems, for example, or to drone-specific regulatory requirements, were excluded because their methodological findings could not be transferred to a general DPIA governance framework without significant context-dependent adaptation that falls outside the scope of this study. Articles that concerned challenges faced by small businesses in complying with the GDPR (DPIA not being the main point) and which lacked a technology focus were also excluded. These were discarded, as the review focuses on DPIA implementation challenges in commercial organisations. Ultimately, 25 studies were included in the sample for the data extraction and analysis.

A data extraction process was adopted to obtain accurate information from the selected sources. Each primary study was carefully read and categorised according to the following variables: Title, Author(s)/Year, Objective, Country/Region Focus, Sector Context, Technology Focus, and Methodology. These items were included to ensure that the data extraction process was consistent with extracting the data elements needed to answer the RQs [20]. As quality assessment is more important in systematic reviews to determine the rigour and appropriateness of primary studies [21], the Critical Appraisal Skills Programme's CASP Systematic Review Checklist [22] was followed for quality assessment. Title and abstract screening and full-text coding were conducted independently by the first and second authors. Disagreements were resolved through discussion until consensus was reached. Formal inter-rater reliability statistics were not calculated; this is acknowledged as a methodological limitation, and future replications of this review are encouraged to report Cohen's kappa or an equivalent reliability measure to strengthen confidence in the thematic synthesis.

Grey literature, including guidance documents from national data protection authorities, supervisory authority opinions, and practitioner publications, was excluded from the SLR corpus. This decision is consistent with established SLR methodology, which priori-

tises peer-reviewed sources to ensure replicability and quality control. It is acknowledged as a limitation; however, the Phase 2 framework partially compensates for this boundary condition, as ISO/IEC 29134:2023 [23]—one of the three reference standards—draws on similar risk assessment principles to those articulated in the WP29 Guidelines on Data Protection Impact Assessment, thereby providing a normative bridge between academic methodology and widely applied supervisory authority guidance.

Framework analysis was used to assess the located sources and address RQ1. This method was selected because it offers a systematic and transparent approach to qualitative analysis and is particularly suitable for applied research with clear research questions and predefined areas of interest [24,25]. This method involves the building of a framework within which emergent themes, in this case DPIA challenges, can be classified or categorised. Goldsmith [26] notes that the method is "an inherently comparative form of thematic analysis which employs an organized structure of inductively- and deductively derived themes (i.e., a framework) to conduct cross-sectional analysis using a combination of data description and abstraction", and that "the overall objective of framework analysis is to identify, describe, and interpret key patterns within and across cases of and themes within the phenomenon of interest" (p. 2061). This analysis of located sources supported the categorization of DPIA challenges in one coherent structure. This is appropriate when a complex phenomenon needs to be organised across several bodies of literature to provide a structure for subsequent research phases. This can be viewed as an initial conceptual framework which Jabareen [27] sees as "a network, or 'a plane,' of interlinked concepts that together provide a comprehensive understanding of a phenomenon or phenomena" (p.51). This definition is relevant to the present study because the use of DPIAs is shaped by the interaction of technological deployment, organisational structuring, regulatory compliance, and process efficiency.

In Phase 2 of the study, the PDCA-based DPIA framework was constructed through a convergent three-source synthesis grounded in independent lines of structural evidence. The first source was inductive: the four-category challenge taxonomy produced by the Phase 1 SLR (legal and regulatory, risk assessment, complexity of implementation, and scope) was analysed to identify which DPIA activities would be required to address each challenge category, with the resulting activity clusters mapped to the Risk Management Domains of the framework (Appendix B, Table A5). The second source was the deductive analysis of the two privacy standards adopted as primary structural references: ISO/IEC 27701:2025 [14], which specifies privacy management system requirements and Annex A controls, and ISO/IEC 29134:2023, which specifies the privacy impact assessment process. The third source was the risk management process specified in ISO 31000:2018 [28], which provides the methodological backbone for both privacy standards and structures risk management into the process steps that constitute the Risk Management Domains of the framework.

The clause-level alignment between each Risk Management Domain and the corresponding clauses of the three standards is documented in Appendix B, Table A4. The convergence of these three independent sources on a comparable phase decomposition provides construct validity for the Risk Management Domain classification. Construct validity here refers to the structural soundness of the framework's design, namely the convergence of independent inductive, deductive, and standards-based sources on a comparable decomposition, and should be distinguished from empirical or predictive validity, which concerns whether the framework produces effective outcomes when applied in practice. The latter is not claimed in this study and constitutes a separate objective for future case study or action research.

This convergent synthesis approach is also consistent with recent studies highlighting the growing overlap between DPIA and Fundamental Rights Impact Assessment (FRIA) obligations under the GDPR [6] and the AI Act [7], and the corresponding need for more harmonised and interoperable impact assessment structures for AI-driven and data-intensive systems [9]. Within each Risk Management Domain, the Control Objectives were derived from the privacy controls and process steps of the two privacy standards, and the Operational Activities were derived through thematic synthesis of the methodological recommendations in the 25 reviewed studies—including CLIFOD [29], PACTS within the TRUSTEE framework [30], the Data Privacy Vocabulary [31], and the Privacy Touch Points framework. This operational structuring also aligns with recent studies examining the variability and practical implementation challenges of DPIA practices across organisations [13]. Each Operational Activity is therefore traceable both to the challenge codes it addresses and to the standard clauses with which it conforms (Appendix B, Table A4), establishing a triple line of evidence for each element of the framework.

3. Results

3.1. Overview of Previous DPIA Studies

The review comprehensively analysed 25 studies, published in peer-reviewed conference proceedings and reputable academic journals. A summary overview of each of these sources is included in Table A2 in Appendix A. Here a synthesis is provided to directly address RQ1.

The majority of DPIA studies are situated within the EU, reflecting the stringent data protection regulations imposed by the GDPR. For instance, studies by Calvi and Kotzinos [32] on AI fairness and those by Grammatopoulos et al. [30] on the TRUSTEE framework demonstrate the EU's leading role in promoting robust data protection measures. Similarly, several studies focus on specific EU member states, such as Germany, with Rehak and Kuhne [33] examining privacy issues in digital contact tracing, and the UK, where Henriksen-Bulmer et al. [29] explore privacy risks in cyber-physical systems. The challenges of risk assessment, notably as regards privacy concerns associated with digital technologies were also examined by Leesakul and Morisset [34]. This highlights the significance of DPIAs in the context of digitalisation as an important component of companies' risk assessment processes.

More specifically, as regards the technology focus, the reviewed literature reveals a strong emphasis on the potential of DPIAs to ensure fairness and accountability, notably in AI systems. Calvi and Kotzinos [32] explore the use of algorithmic impact assessments, including DPIAs, to protect individuals from algorithmic harm by assessing the societal impacts of AI systems. Their research highlights the need to bridge legal, social and computer science domains to develop fairer AI solutions within regulatory frameworks. Two studies conducted by Papamartzivanos et al. [35] and Janssen et al. [36] not only investigated DPIA applications in the context of ICTs/AI but also provided guidance on the complexity and scope of DPIA implementation in combination with these technologies. They provide a dynamic and generic assessment process by addressing the Automated Privacy and Security Impact Assessment (APSIA) methodology, which combines privacy and security impact assessments using interdependency graph models and data processing flows to quantify the privacy risks posed by vulnerabilities, and the Fundamental Rights Impact Assessment Framework (FRIAF), which allows organisations to systematically assess the potential impact of AI systems on fundamental rights.

Similarly, Moniz [37] emphasises that, in the context of AI systems, DPIAs require data controllers to perform complex balancing and proportionality assessments to safeguard fundamental rights, highlighting the structural risks of subjectivity and inconsistency in

these evaluations. To address these challenges, Moniz [37] further argues that fundamental rights considerations may require dedicated and more structured assessment mechanisms alongside the DPIA to ensure greater consistency and transparency in high-risk AI contexts. Rintamäki et al. [9] further examine the overlap between DPIA requirements under the GDPR and FRIA obligations under the AI Act, highlighting the need for more harmonised impact assessment approaches for AI systems involving personal data. The applicability of DPIA in IoT systems and smart cities has been explored in various studies, such as that of Campanile et al. [38], who investigate how blockchain technology can enhance privacy and GDPR compliance in IoT systems, particularly in the context of the Internet of Vehicles (IoV). Their research aims to create trusted data recording systems that improve road safety and legal accountability.

López et al. [39] propose adapting DPIA as a legal methodology to assess privacy by design in identity management technologies, emphasising the importance of considering both architectural and user aspects to address the challenges of digital identity management. Georgiadis and Poels [3] focus on DPIA methodologies in the context of big data analytics. Their research aims to develop a comprehensive DPIA framework to identify, analyse and mitigate privacy risks specific to big data environments. In a subsequent study, Georgiadis and Poels [40] examine the limitations of existing GDPR-aligned DPIA frameworks, noting that they often fail to adequately capture big-data-specific risks such as unclear controllership, re-identification threats, discrimination concerns, transparency limitations and challenges in stakeholder involvement, thereby highlighting the need for a refined and operationalised methodology tailored to big data analytics contexts. The IT sector features prominently in many DPIA studies, reflecting the pervasive nature of technology and the privacy challenges it poses. This is evident in Mantelero's [41] research on AI and big data, which highlights the intersection of IT with human rights and ethical considerations. The integration of IT with healthcare is another critical area, highlighted by Papamartzivanos et al. [35], who discuss the convergence of privacy and security impact assessments within healthcare IT infrastructures. These studies highlight the diverse applications of DPIA in different technological contexts, demonstrating its critical role in ensuring privacy and compliance in environments where AI, IoT, big data, and blockchain technologies introduce high-risk data processing activities.

The technological focus thus varies across studies, with significant attention paid to primary digital technologies: AI, analytics and big data, blockchain, and IoV. Other notable technology focuses include smart building technologies, as explored by Leesakul and Morisset [34], and biometric authentication systems, as explored by Bisztray et al. [42]. Similarly, Gültekin-Várkonyi [43] identifies facial recognition technologies as a key privacy concern, highlighting the specific risks they pose to data minimisation, purpose limitation, system accuracy, and administrative challenges under the GDPR and AI Act.

The methodologies used in these studies range from conceptual frameworks to mixed methods approaches. Conceptual methods are used to develop theoretical models and frameworks, as in the studies by López et al. [39] on DPIA methodologies and Pandit [31] on semantic specifications for DPIAs. Mixed methods approaches are also common, combining theoretical analysis with practical application, as seen in the work by Henriksen-Bulmer et al. [29] on cyber-physical systems and by Riemann et al. [44] on open-source software tools for DPIAs. Wright and Hert [45] emphasise the critical role of combining theoretical insights with practical applications to develop robust privacy frameworks. This approach is further supported by Johnson and Onwuegbuzie [46], who emphasise that mixed methods research provides a richer understanding of research problems by integrating both qualitative and quantitative data.

Qualitative approaches are also used to provide in-depth insights, such as in Vemou and Karyda's [47] study on the evaluation of privacy impact assessment methodologies. Bryman [48] highlights the importance of qualitative research in providing a rich and detailed understanding of social phenomena. He discusses how qualitative methods are particularly effective in exploring complex and nuanced issues and underscores that integrating qualitative approaches with quantitative data can lead to more comprehensive insights, enabling a fuller understanding of the phenomena under study. Additionally, other important studies emphasise the significance of these methods in DPIA research. Wright and Hert [45] highlight the critical role of DPIAs in identifying and mitigating privacy risks within organisational processes, supporting regulatory compliance, and enhancing stakeholder trust. Their work highlights the importance of conceptual methodologies in developing robust privacy frameworks. Furthermore, Bieker et al. [49] researched the application of DPIAs in the context of smart grids, illustrating the effectiveness of qualitative methods in understanding the nuanced privacy implications of emerging technologies. Similarly, Gültekin-Várkonyi [43] demonstrates that DPIAs are pivotal in evaluating and mitigating the legal, technical and administrative risks associated with facial recognition technologies, reinforcing regulatory compliance and supporting public trust in high-risk biometric surveillance contexts. Their findings underscore the importance of qualitative approaches in providing detailed insights into privacy risks and stakeholder concerns.

Collectively, previous DPIA studies encompass a wide range of technologies and business environments, highlighting the versatility and necessity of DPIAs in various domains. This underlines the importance of adapting DPIA methodologies to specific industry needs and technological contexts to ensure robust privacy and data protection measures in different applications.

3.2. RQ1. What Challenges Were Encountered in Implementing the DPIA, Particularly in the Area of Technology-Based Data Processing?

The reviewed literature contained relatively little content regarding the challenges of implementing DPIA in the corporate environment in the context of rapid digitalisation. Nevertheless, four recurring categories of challenges can be identified across the reviewed corpus: legal and regulatory challenges, risk assessment challenges, complexity of DPIA implementation, and enhancing the scope of DPIAs. Given the focused evidential base of 25 studies, these categories should be understood as a structured synthesis of the challenges recurring in the reviewed literature rather than an exhaustive account of the entire DPIA challenge landscape.

Legal and regulatory challenges include navigating different and sometimes conflicting privacy laws in different jurisdictions, which can complicate compliance efforts. Risk assessment challenges include the difficulty of identifying, assessing and mitigating privacy risks, particularly in complex data ecosystems where data flows across multiple platforms and stakeholders. The complexity of DPIA implementation is another significant barrier, involving the need for multidisciplinary expertise, the integration of technical and organisational measures, and aligning DPIA processes with overall business objectives. Finally, enhancing the scope of DPIAs to keep pace with emerging technologies and evolving privacy concerns is essential to ensure that privacy protections are robust and comprehensive.

Although the four categories are analytically distinct, the boundary between risk assessment and implementation complexity warrants clarification, as both concern the challenges of conducting DPIAs. Risk assessment challenges (R1–R7) address the substantive nature of GDPR privacy risk: it differs from traditional risk management in its object (rights and freedoms of data subjects), its required perspective (data-subject-centred assessment), and its quantification logic (contextual proportionality rather than actuarial

probability). Implementation complexity challenges (C1–C15) concern the operational and organisational conditions required to execute a DPIA in practice, including interdisciplinary coordination, integration of technical and legal expertise, tooling gaps, and documentation governance. On this basis, challenges such as C12 (complexity of calculating risk scores) and C14 (difficulty of applying DPIAs in big data analytics environments) are classified as complexity challenges because they address procedural execution barriers, not the substantive character of the risk itself. This distinction is further reflected in the Phase 2 framework, where R codes map primarily to the Risk Identification and Impact Evaluation domain, while C codes distribute across multiple domains given their cross-cutting operational character (Table A6, Appendix B).

These four challenge categories are now examined in more detail.

3.2.1. Legal and Regulatory Challenges

The implementation of DPIAs in the face of technological developments poses significant legal and regulatory challenges (Table 2). These challenges include the varied interpretation of high-risk processing activities that necessitate a DPIA, the potential for circumvention when AI systems claim to process synthetic or anonymous data, and the lack of consistent guidance from regulators and courts regarding the application of fairness metrics within DPIAs. This complexity is further exacerbated by differing responsibilities and oversight mechanisms across these assessments, which can lead to legal uncertainties and compliance difficulties for entities deploying AI systems [32]. Recent research further demonstrates that the overlap between the GDPR [6] and the AI Act [7] creates additional regulatory fragmentation and compliance uncertainty regarding high-risk AI systems and impact assessment obligations. In particular, significant divergences persist across EU/EEA member states concerning DPIA-triggering criteria, sector-specific high-risk categorizations, and the interpretation of processing activities requiring impact assessments, thereby complicating the harmonisation and operational implementation of DPIAs and FRIAs across jurisdictions [9]. In addition, Campanile et al. [50] highlighted that one of the biggest challenges for security and privacy assurance in IoT systems is the introduction of privacy regulations and the development of robust and secure solutions for data management. Accordingly, they emphasised that despite existing cybersecurity architectures, IoT systems remain vulnerable to security issues such as unauthorised access, data breaches, and intrusions, and thus, data-centric and IoT systems are strongly affected by these regulations, and fully adequate solutions have yet to be designed.

Table 2. DPIA legal and regulatory challenges.

• Lack of a legal obligation for organisations for AI-based business models (L1) • Customising DPIA methodology to business environment. Whilst area or sector-specific DPIA methodologies have been developed, most of the existing widely used methodologies are context-independent and significant divergences across EU/EEA member states regarding DPIA-triggering criteria and high-risk categorizations create additional harmonisation and compliance challenges for AI systems (L2) • Solutions for large-scale digital systems and services, such as those based on IoT, are not yet properly designed to comply with privacy requirements (L3)	Rintamäki et al. [9] Calvi and Kotzinos [32] Bisztray et al. [42] Campanile et al. [50]

3.2.2. Risk Assessment Challenges

The literature review reveals a variety of challenges in conducting risk assessments, including managing complex interactions between different stakeholders, data sharing, and processing, which can lead to a lack of control over access points and increased security risks. Leesakul and Morisset [34] identify significant risk assessment challenges

in implementing DPIAs in smart buildings, focusing on the technological aspects. Accordingly, a key challenge is that the factors contributing to high risk under GDPR differ from traditional risk management. Traditional risk management primarily focuses on technical threats and vulnerabilities, whereas the GDPR emphasises the potential impact on individual rights and freedoms. This shift requires a broader and more nuanced approach to risk assessment, integrating legal, ethical and social dimensions alongside technical considerations. Moreover, Gültekin-Várkonyi [43] shows that similar challenges arise in the context of facial recognition technologies, where organisations must assess risks linked to data minimisation, purpose limitation, biometric accuracy and administrative gaps under both the GDPR and the AI Act. Henriksen-Bulmer et al. [29] also referred to the traditional risk management emphasised by Leesakul and Morisset [34]. Henriksen-Bulmer et al. [29] additionally introduced the Contextual Integrity for Open Data (CLIFOD) pilot study, which provides a risk assessment framework based on Contextual Integrity (CI). The CLIFOD framework employs three overarching phases: explanation, risk assessment, and decision. This structured approach helps decision-makers evaluate privacy risks by considering the specific context and processing practices involved. The phases guide users in understanding existing practices, assessing the risks associated with any changes, and making informed decisions based on the potential consequences of those changes. This framework is designed to aid organisations in assessing privacy from both the organisation's and the individual's perspectives, facilitating GDPR compliance. DPIA risk assessment challenges are given in Table 3.

Table 3. DPIA risk assessment challenges.

• Factors contributing to high risk under GDPR differ from traditional risk management (R1) • The complexity of interaction between different actors, data sharing and processing leads to a potential lack of control over the management and monitoring of access points, making the building system more prone to security risks and vulnerabilities (R2) • The complexity of assessing risks such as unauthorised access to personal data, data alteration and data loss (R3) • The comprehensive identification of potential privacy risks requires coverage of both the physical and technological processes and the systems through which data passes as part of the analysis (R4) • The requirement for organisations to assess risks from the perspective of the data subject, rather than from the perspective of the organisation, as is traditionally the way businesses assess risk (R5) • Requirement for a privacy risk assessment that will allow the organisation to assess the privacy impacts of data processing on its customers in a consistent, repeatable manner (R6) • The difficulty of assessing risks in facial recognition systems due to challenges such as ensuring data minimisation, defining and limiting purposes, verifying the accuracy of biometric data, and addressing administrative and accountability gaps under the GDPR [6] and the AI Act [7] (R7)	Leesakul and Morisset [34] Henriksen-Bulmer et al. [29] Gültekin-Várkonyi [43]

3.2.3. Complexity of DPIA Implementation Challenges

As a third challenge factor, the complexity of DPIA implementation has been discussed extensively in the literature, as shown in Table 4. The implementation of DPIAs faces many challenges, including the need for a holistic, user-centred assessment matrix that captures technical, legal and socio-ethical dimensions; integration with cybersecurity metrics; thorough understanding of technical and legal requirements; interdisciplinary collaboration; and the complexity of risk identification, assessment and mitigation, particularly in net-

worked projects in the health sector. In AI-driven healthcare contexts, these challenges are further intensified by the need to operationalise meaningful human oversight, align DPIAs with FRIAs, and integrate accountability, governance and lifecycle monitoring requirements into clinical workflows [51]. In this regard, Grammatopoulos et al. [30] highlight several complexities in conducting DPIAs in the digital age. One major complexity is the need for a holistic, user-centred assessment that integrates technical, legal, ethical and social dimensions, making the DPIA process inherently complex. The need for rigorous risk assessments to identify potential breaches of personal rights and propose mitigation strategies further complicates the process. Compliance with GDPR obligations, as well as the protection of individual rights, requires a deep understanding of data processing activities. The TRUSTEE framework addresses these challenges with its Application Building Blocks (ABBs), in particular the DPIA ABB, which uses the comprehensive Privacy and Security Assessment for Cross-discipline Trust and Sovereign (PACTS) methodology. This structured, iterative approach ensures careful handling of personal data, ongoing stakeholder engagement and thorough evaluation of risk mitigation strategies. In line with these complexities, Moniz [37] further demonstrates that DPIA implementation also involves substantial interpretative challenges, as data controllers must conduct balancing and proportionality assessments that are inherently subjective, raising concerns about consistency, legitimacy and the overall reliability of DPIA outcomes.

Table 4. DPIA implementation complexity challenges.

• The need for a holistic assessment matrix that is user-centred, captures technical, legal and socio-ethical dimensions, and provides a comprehensive approach to privacy (C1). • The necessity of integration with cybersecurity metrics that combine security and privacy concerns in data protection efforts (C2). • The necessity for assessments to involve the entire process, including servers, network infrastructure or operating system frameworks, or even parts of the process that do not use technology (C3). • The need for a thorough understanding of both the technical aspects of the technology and the legal requirements of data protection regulations such as GDPR (C4). • The necessity for legal experts to discuss with subject matter experts the technical feasibility of the proposed protection measures/possible adaptations or modifications to which these measures may be subjected (C5). • Obstacles to incorporating the principle of fairness into the DPIA process, including the difficulty of determining what qualifies as fair processing and how to balance conflicting rights and interests (C6). • The necessity to establish a direct link between data processing flows and the organisation's current state of cybersecurity in order to determine the magnitude of privacy risks beyond the documentation of an organisation's data and procedures (C7). • Analysing privacy impact from an organisational or individual perspective, identifying metrics used to measure privacy risks and risk mitigation strategies (C8). • The interdisciplinary nature of the DPIA, not only due to the technical and multifaceted nature of the task, but also due to the legal, organisational, medical and IT aspects, particularly in AI-driven healthcare environments requiring meaningful human oversight, FRIA-DPIA alignment and governance integration into clinical workflows (C9). • The collaborative effort required to bring together expertise and integrate different perspectives in a coherent way is time-consuming and complicated (C10). • Lack of an open-source framework to facilitate the DPIA process, especially for complex, networked projects in the health sector (C11). • The complexity of the processes of identifying risk sources, subdividing them into groups, calculating risk scores based on probability and potential harm, formulating TOMs and re-evaluating risks after the implementation of TOMs (C12). • Complexity of processes for stakeholders to identify relevant risks and mitigations for special considerations in impact assessments, emerging technologies and use cases, and to document results in a coherent manner, particularly due to heterogeneous DPIA practices, ad hoc methods and insufficiently assessed multi-stakeholder processes (C13). • The difficulty of applying DPIAs in big data analytics environments, where interdependent risks such as re-identification, discrimination, opacity of processing and unclear controllership require the integration of legal, technical, organisational and societal considerations into a single coherent assessment process (C14). • The challenge of ensuring consistent, legitimate and non-subjective DPIA outcomes, given that balancing and proportionality assessments rely heavily on discretionary judgement by data controllers (C15).	Lazcoz et al. [51] Hansen et al. [13] Grammatopoulos et al. [30] Rehak and Kuhne [33] López et al. [39] Kasirzadeh and Clifford [52] Campanile et al. [50] Papamartzivanos et al. [35] Vemou and Karyda [47] Riemann et al. [44] Pandit [31] Georgiadis and Poels [40] Moniz [37]

On the other hand, López et al. [39] highlighted in their study that one of the main challenges is the collaborative effort required to bring together expertise from different fields, including technical, legal and institutional perspectives. Hansen et al. [13] further suggest that DPIA implementation practices remain heterogeneous across organisations, with handwritten DPIA reports, ad hoc methods, and insufficiently assessed multi-stakeholder processes still characterising practical implementation approaches. This multidisciplinary integration is time-consuming and complex, as it requires harmonising different levels of understanding and experience among stakeholders to ensure a coherent approach to risk assessment and privacy protection and emphasises that effective collaboration between technical and legal experts is essential to address the multifaceted nature of data protection and to ensure a comprehensive consideration of all aspects of privacy by design.

Pandit [31] addresses the complexity of DPIA implementation in the digital age, highlighting the necessity of a holistic and structured approach to risk management. Meanwhile, Kasirzadeh and Clifford [52] emphasise that the fairness metrics of DPIA implementation can improve decision-making by providing a structured approach to assessing the impact of data processing on individuals' rights and freedoms. In this regard, Pandit [31] emphasises the need to develop an ontology based on ISO 31000 standards, arguing that it increases the effectiveness and consistency of DPIA by helping to systematically identify and address risks while Kasirzadeh and Clifford [52] provide fairness criteria to identify and reduce biases in automated decision-making processes, prevent biassed or unfair outcomes, provide a concrete and workable framework for assessing fairness, and guide the data controller through the challenges in this regard.

3.2.4. Enhancing DPIA Scope Challenges

Lastly, focusing on enhancing the scope of DPIAs, Mantelero [41] underlined that technological developments require a broader and more comprehensive approach to DPIAs and that the increasing capacity for data processing and analysis requires DPIAs to have a more holistic perspective, covering not only the technical and legal aspects but also the social and ethical impacts of data processing activities, and emphasised the importance of this holistic perspective for identifying and mitigating potential risks associated with AI, big data technologies. Similarly, Georgiadis and Poels [3] argue that traditional DPIA frameworks are ill-equipped to deal with the complexities of big data. In particular, they highlight that the nature of big data processing, which often involves large-scale data processing, extensive profiling and the combination of different data sets, makes it difficult to assess privacy risks and identify high-risk processing activities. In this context, the lack of clear guidelines and concrete requirements for conducting DPIAs increases uncertainty and the difficulty of ensuring comprehensive data protection.

Based on the findings discussed in the literature review, it can be concluded that the implementation of DPIAs faces significant challenges due to the rapid advancement of AI and big data technologies. Legal and regulatory gaps, inadequate practical guidance and the complexity of risk assessment from the data subject's perspective are major hurdles. In addition, the need for a holistic, interdisciplinary approach and the integration of cybersecurity metrics complicate DPIA processes. Broadening the scope of DPIA by including marginalised groups and addressing big data-specific risks is essential. Addressing these challenges will ensure effective and comprehensive data protection practices in the digital era and promote ethical and fair decision-making in data processing activities. Continued efforts to refine DPIA methodologies will be crucial to adapt to evolving technological landscapes. DPIA scope-related challenges are given in Table 5.

Table 5. DPIA scope-related challenges.

• Involvement of women or other marginalised groups in the DPIA process to better identify risks/measures to rights and freedoms arising from processing activities (S1). • The inclusion of mobility data in data processing operations poses particular challenges for the protection of ethical principles and makes the operation more elaborate (S2). • The necessity to develop broader forms of data protection impact in processes dominated by the widespread use of Big Data analytics, algorithms and AI (S3). • Lack of materials in an accessible format detailing what fundamental rights exist in organisations and how they relate to and can be affected by AI systems (S4). • The necessity for a comprehensive methodology that is more appropriate to the privacy and data protection risks in environments where big data is stored and Big Data Analytics algorithms are applied (S5).	Calvi [53] Jong et al. [54] Janssen et al. [36] Georgiadis and Poels [3]

The overall categorisation of DPIA challenges identified through the literature review is summarised in Figure 3.

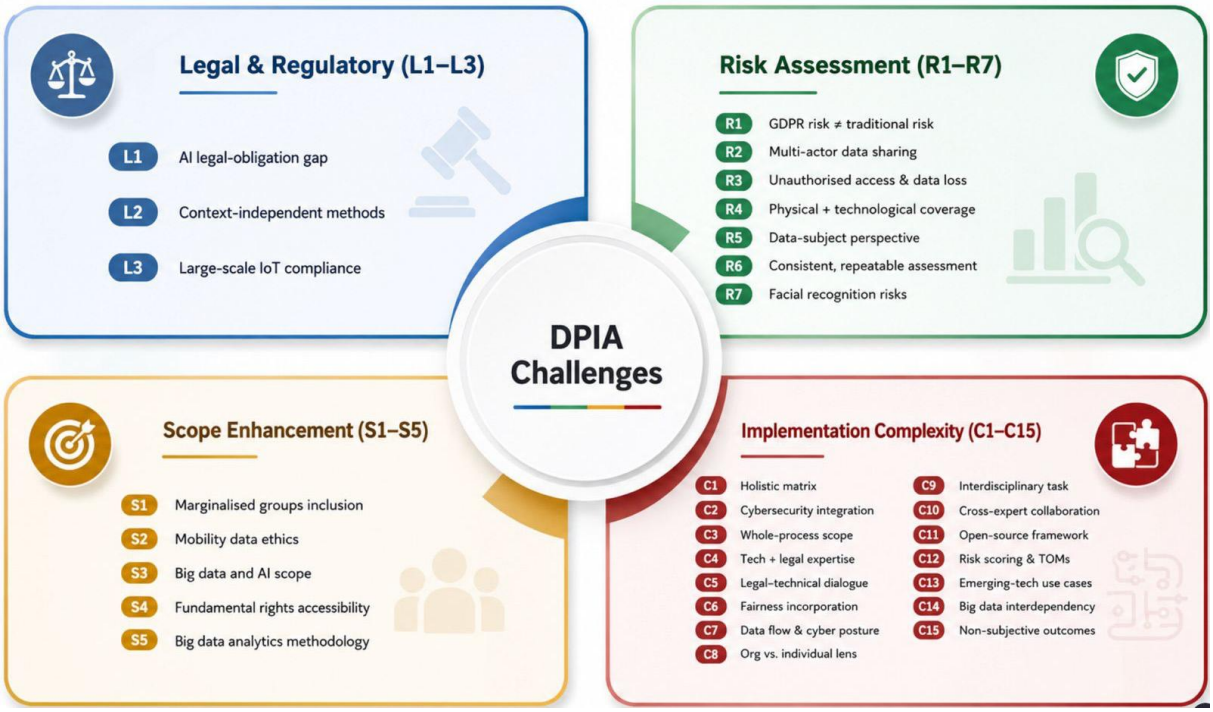

Figure 3. Categories of DPIA challenges.

Tables 2–5 provide a more detailed listing of challenges pertaining to each of the four categories. This constitutes the Provisional Conceptual Framework (PCF) for the subsequent development of an operational framework to address the various hurdles associated with conducting a DPIA. The mapping between each identified challenge and the corresponding risk mitigation activities proposed in the Phase 2 framework is documented in Appendix B (Tables A3–A6), which provide challenge-level traceability across the framework's Operational Activities and their grounding in the three reference standards. By systematically addressing each of these challenges, organisations can improve their privacy practices, better comply with regulatory requirements, and ultimately protect the privacy of individuals in an increasingly data-driven world.

The translation from the Phase 1 challenge taxonomy to the Phase 2 framework activities followed a structured four-step procedure. First, each challenge category was reviewed to determine the type of DPIA capability required to address it: legal and regulatory challenges implied a need for compliance verification activities; risk assessment

challenges implied a need for structured risk identification and impact evaluation; complexity challenges implied a need for operational governance mechanisms addressing coordination, documentation, and process structuring; and scope challenges implied a need for contextual scoping and adaptive review. Second, the resulting capability clusters were assigned to PDCA lifecycle phases based on their temporal logic: risk identification and scoping activities to the Plan phase, mitigation and documentation activities to the Do phase, monitoring and compliance verification to the Check phase, and adaptive responses to emerging technologies to the Act phase. Third, the inductive activity clusters were cross-checked against the deductive structure of the three reference standards—ISO 31000:2018, ISO/IEC 27701:2025, and ISO/IEC 29134:2023—to establish standard-level traceability for each activity. Where the three sources converged on a comparable phase decomposition, a Risk Management Domain was confirmed; where the standards provided no explicit guidance—particularly regarding algorithmic fairness, broader socio-ethical impact, and adaptation to emerging technologies—the framework extended them in alignment with the EU AI Act Article 27 FRIA requirement. Fourth, each Operational Activity was assigned one or more challenge codes (L, R, C, S) to make the mapping between empirically identified challenges and proposed framework components explicit and auditable. This mapping is documented in Table A6 (Appendix B) and visualised in Figure 4.

3.3. RQ2. Can a Framework Be Developed to Address the DPIA Implementation Challenges for Digital Technologies?

The increasingly wide deployment of rapidly evolving digital technologies has introduced new complexities and risks to data protection that traditional DPIA frameworks may not adequately address. Wright and Hert [45] discussed the need for DPIA frameworks to evolve in response to the dynamic nature of technology and the increasing volume of data being processed by emphasising the importance of adapting existing methodologies to take account of new privacy risks and regulatory requirements. The integration of fairness metrics [55] provides a structured approach to assessing the impact of data processing on individuals' rights and freedoms. These metrics can improve decision-making processes and help mitigate bias in automated systems, ensuring that DPIAs not only meet legal standards but also adhere to ethical principles. In line with this perspective, Calvi and Kotzinos [32] argue that impact assessment frameworks should explicitly embed fairness analysis into the DPIA process by operationalising group and procedural fairness metrics, thereby strengthening the evaluation of algorithmic decision-making systems and enhancing the overall socio-ethical robustness of DPIAs. The need for a holistic assessment matrix that captures technical, legal and socio-ethical dimensions is highlighted by Binns [56], who proposes the development of comprehensive risk assessment frameworks tailored to the specific challenges of emerging technologies. Such frameworks facilitate the systematic identification and mitigation of risks, thereby increasing the overall effectiveness of DPIAs.

Georgiadis and Poels [3], however, argue that there is a significant lack of consensus on a consistent methodology for conducting DPIAs, particularly in the context of big data analytics. They highlight that current research does not provide clear guidelines or standardised approaches for effectively addressing privacy and data protection risks in this area. The authors note that existing PIA methodologies, which have been adapted to meet DPIA requirements under the GDPR, show significant variability in scope and detail. In support of this perspective, other researchers have also noted the lack of a standardised DPIA methodology. Custers et al. [57] point out that the different interpretations of GDPR requirements in different jurisdictions lead to inconsistencies in how DPIAs are conducted. Similarly, Bieker et al. [49] highlight that the lack of a consistent approach makes it difficult for organisations to implement effective data protection measures, as they have to navigate different, often conflicting, guidelines. These inconsistencies can lead to inadequate risk

assessments and undermine the effectiveness of DPIAs in protecting personal data. The literature consistently calls for the development of a harmonised DPIA framework that can provide clear, actionable guidance to organisations across sectors and geographies.

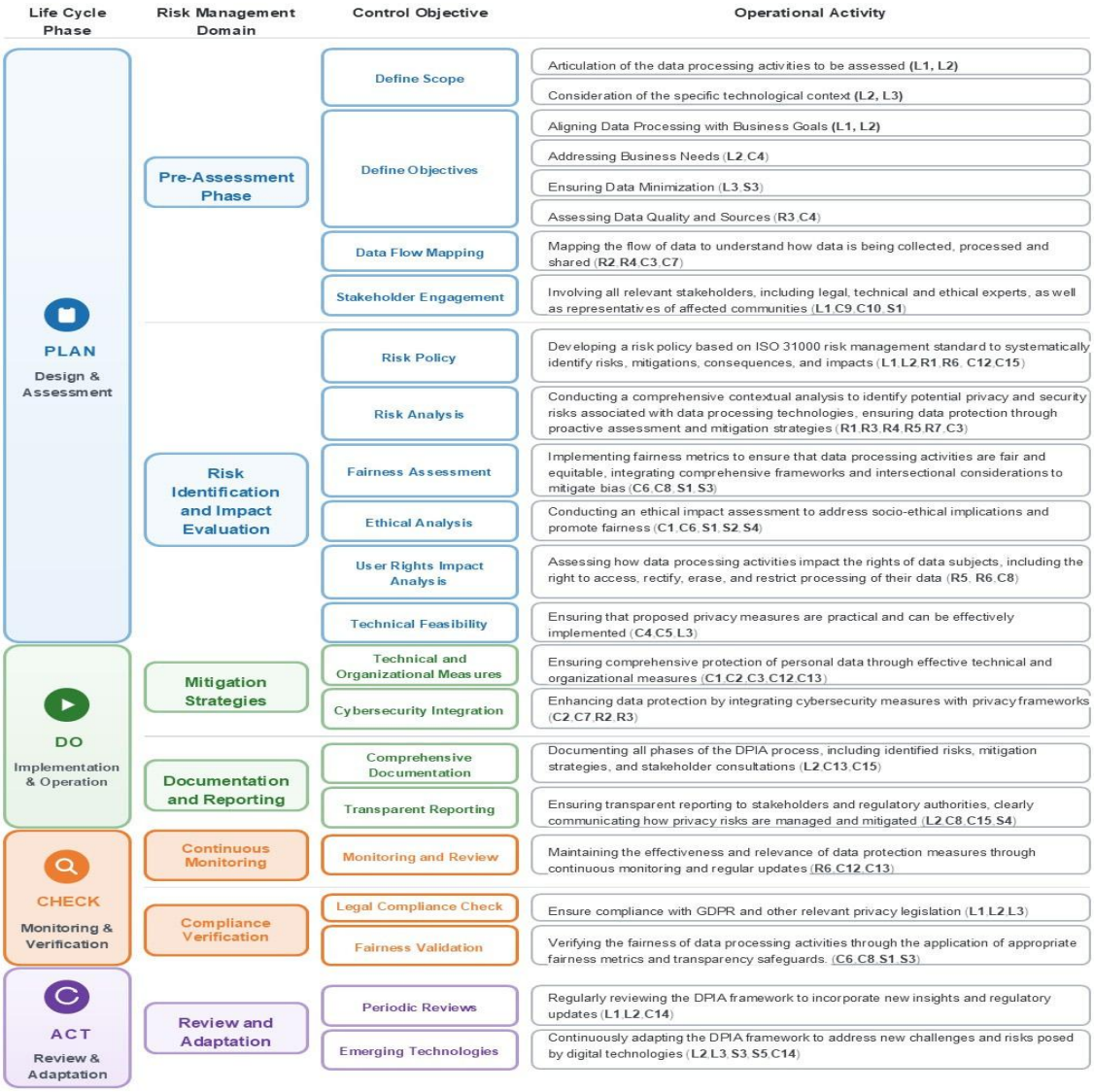

Figure 4. Comprehensive PDCA-based DPIA framework for AI-Driven Digitalisation. (The figure indicates the linkage across the four stages of the framework. The columns from left to right are: Lifecycle Phase → Risk Management Domain → Control Objective → Operational Activity. In the Operational Activity stage, the addressed challenges are shown in parentheses).

The inconsistency of DPIA methodologies is further evidenced in various academic studies, which highlight the need for a more harmonised framework to guide organisations in the effective implementation of DPIAs. Existing studies further indicate that DPIA practices are still largely shaped by fragmented and organisation-specific implementation approaches, limiting methodological consistency and the systematic assessment of complex processing activities [13]. The included studies collectively highlight the need for updated DPIA frameworks that can address the unique challenges of emerging technologies, ensure robust data protection, and comply with regulations such as GDPR. Addressing these complexities requires interdisciplinary collaboration, integration of cybersecurity metrics, and continuous adaptation of best practices to keep pace with technological advances. Recent studies further indicate that effective DPIA implementation in AI-supported environ-

ments also requires operational governance mechanisms capable of supporting meaningful human oversight, continuous monitoring and workflow-integrated safeguards [51]. By harmonising DPIA methodologies, organisations can better navigate the diverse legal and regulatory landscape, improve their risk assessment processes, and manage the inherent complexity of DPIA implementation in a rapidly evolving technological environment.

To address this gap in practice and academic literature, a technology-oriented DPIA methodology is proposed to address the unique challenges posed by digital technology deployment. This methodology integrates technical, legal, and socio-ethical dimensions to provide a comprehensive risk assessment framework. By incorporating fairness metrics, ensuring continuous monitoring and adaptation, and promoting interdisciplinary collaboration and stakeholder engagement, the framework aims to enhance the effectiveness and robustness of DPIA processes.

The proposed framework addresses the four challenge categories identified in Phase 1 by structuring operational activities across the PDCA lifecycle. Legal and regulatory challenges are addressed primarily through the Compliance Verification domain in the Check phase, with support from the Pre-Assessment Phase's scoping activities. Risk assessment challenges are addressed through the Risk Identification and Impact Evaluation domain in the Plan phase, with its decomposition grounded in ISO 31000 risk management principles to address the Phase 1 finding that GDPR risk differs from traditional risk management. Complexity challenges are addressed cross-cuttingly: methodological complexity is reduced by the four-level hierarchy itself; collaboration complexity is addressed by continuous Stakeholder Engagement; and documentation complexity is addressed by the Documentation and Reporting domain. Scope challenges are addressed through Pre-Assessment Phase scoping and through the Emerging Technologies activity of the Act phase, which provides dedicated operational treatment for adapting the framework to evolving digital technology contexts. The complete mapping of challenge codes to Risk Management Domains is documented in Table A5 (Appendix B), and Figure 4 annotates each Operational Activity with the specific challenge codes it addresses, providing a direct visual mapping from the empirically identified challenges to the proposed framework components.

Within the Risk Policy domain, the specific ISO 31000:2018 operationalised elements are in the following sections of the standard: Section 5.4.2 (establishment of an organisational risk management policy as a governance commitment); Section 6.3.4 (definition of risk criteria, i.e., the thresholds and standards against which the significance of privacy risk is evaluated); Section 6.4.2 (risk identification, covering the systematic discovery of risk sources, events, and consequences relevant to the processing activity); and Section 6.4.4 (risk evaluation, comprising the comparison of risk analysis results against the defined criteria to support prioritisation decisions). The domain label Risk Policy is therefore used in the sense of ISO 31000. Section 5.4.2 governance mandate, while its operational activities implement the Section 6 process steps. An illustrative application of the framework to an AI-based recruitment screening system, including an operationalised example of fairness metric selection, is provided in Appendix C.

The proposed DPIA methodology is structured around the Plan–Do–Check–Act (PDCA) cycle to ensure methodological coherence and a continuous improvement logic. This structure reflects the governance model adopted in ISO/IEC 27701 and ISO/IEC 29134, which aligns privacy management with other management system standards by embedding iterative monitoring, performance evaluation, and adaptive review mechanisms. Applying the PDCA cycle transforms the DPIA into a recurring process rather than a one-time assessment, supporting periodic re-evaluation of privacy risks, verification of compliance, and the adaptation of mitigation measures to emerging technological developments. This approach strengthens organisational resilience, integrates DPIA practices

into broader information security governance, and provides a transparent structure for traceability and accountability in risk-based decision-making.

The framework's construct validity is supported by four complementary mappings detailed in Tables A3–A6 in Appendix B, each independently grounding a different dimension of the framework's structure (Table 6).

Table 6. Four complementary mappings supporting the construct validity of the proposed framework.

Table	Mapping Direction	Source of Evidence	Validity Dimension
Table A3	Operational Activity → Literature source	Phase 1 SLR (25 reviewed studies and supplementary sources)	Inductive grounding
Table A4	Operational Activity → Standard clause	ISO 31000:2018, ISO/IEC 27701:2025, ISO/IEC 29134:2023	Deductive grounding
Table A5	Challenge category → Risk Management Domain	Phase 1 challenge taxonomy	Convergent construct validity
Table A6	Challenge category → Operational Activity	Phase 1 challenge taxonomy and coding with the corresponding PDCA Phase and Risk Management Domain.	Convergent construct validity

Figure 5 illustrates the cyclical nature of the DPIA Framework for digital technologies, which is structured around the PDCA approach to ensure iterative assessment and continuous improvement. Lifecycle Phase and Risk Management Domains based on ISO 31000 are shown in Figure 5 for clarity. The Control Objective and Operational Activity levels are shown in Figure 4, which also indicates the specific challenges addressed by operational activities. A detailed description of each Lifecycle Phase, Risk Management Domains, Control Objectives, and Operational Activity descriptions with supporting literature sources, is provided in Table A3 in Appendix B.

The framework integrates technical, legal, and socio-ethical dimensions to provide a thorough risk assessment approach, structured in accordance with the PDCA cycle. By incorporating fairness metrics, ensuring continuous monitoring and adaptation, and promoting interdisciplinary collaboration and stakeholder engagement, the framework aims to enhance the robustness and effectiveness of DPIA processes, and to effectively address the challenges posed by digitalisation identified in response to RQ2. It is designed to help organisations navigate the complexities of data protection in the digital age, ensuring compliance with the GDPR and other relevant regulations, and provides a structured approach to identifying and mitigating data protection risks associated with the rapid evolution of technology.

The DPIA framework consists of four phases that comply with the PDCA cycle, allowing organisations to plan and assess risks (PLAN), implement mitigation measures (DO), verify and monitor the effectiveness of controls (CHECK), and iteratively update their DPIA approach in response to technological change and new regulatory guidance (ACT). The pre-assessment phase includes defining the scope of data processing activities, setting objectives aligned with business objectives, mapping data flows, and engaging stakeholders. The Risk Identification and Impact Evaluation phase includes developing a risk policy, conducting a comprehensive risk analysis, applying fairness assessment frameworks, conducting ethical impact assessments, performing a user rights impact analysis, and examining the technical feasibility of proposed measures. This phase ensures that privacy risks, socio-ethical considerations, fairness implications, individual-level impacts and technological constraints are systematically identified and assessed prior to decision-making. The Mitigation Strategies phase focuses on implementing technical and organisational measures, integrating cybersecurity practices, assessing technical feasibility, and establishing continuous monitoring and review mechanisms. The Documentation and Reporting phase emphasises comprehensive documentation and transparent reporting to stakeholders. Finally, the Review

and Adaptation phase calls for periodic review and adaptation to emerging technologies. This structured and holistic approach aims to provide organisations with the tools they need to effectively manage privacy risks in the face of rapidly evolving technologies. The full framework stages, such as lifecycle phase, GRC domain, Control Objectives, and Operational activities, are presented in Table A3 (Appendix B). Furthermore, Table A4 complements Table A3 by mapping each operational activity of the proposed PDCA-based DPIA framework (Figure 4) to the corresponding clauses of three international standards: ISO 31000:2018, which provides the risk management process backbone; ISO/IEC 27701:2025, which specifies Privacy Information Management System (PIMS) requirements and ISO/IEC 29134:2023. Table A5 in Appendix B documents the mapping between the Phase 1 challenge taxonomy and the Risk Management Domains of the framework, showing how each challenge category was operationalised into one or more domains.

Figure 5. Plan-Do-Check-Act-based DPIA framework for AI-Driven Digitalisation (Risk Management domains are shown in each PDCA lifecycle phase).

In addition, the details provided at each phase of this DPIA framework are particularly valuable for companies operating technology-driven data processing processes to implement DPIAs. These details provide practical guidance on various aspects of the DPIA process, helping organisations to effectively manage privacy risks and ensure compliance with data protection regulations. By following the steps outlined in this framework, organisations can systematically identify and address privacy risks and ensure that their data processing activities comply with both legal requirements and ethical standards. The integration of technical, legal, and socio-ethical considerations ensures that all aspects of data protection are covered, providing a holistic approach to managing privacy risks. By adopting this comprehensive framework, organisations can improve their risk assessment processes, better manage the inherent complexities of DPIA implementation, and ultimately enhance the protection of individuals' rights and freedoms in the context of digitalisation.

4. Discussion

AI is reshaping how organisations think about data protection, and the regulatory environment is making significant progress and closing the gap rapidly. The EU AI Act expands the concept of risk management and introduces a new obligation, the FRIA under Article 27, which complements the DPIA already required under Article 35 of the GDPR. Taken together, a standalone DPIA may not be sufficient for high-risk AI deployments. Our findings reflect this shift directly. The challenge taxonomy developed in Phase 1 captures several AI-specific barriers, including the absence of a legal obligation for AI-based business models (L1), governance risks around facial recognition under the GDPR [6] and the AI Act [7] (R7), and the lack of accessible guidance on AI's impact on fundamental rights (S4). These are not abstract concerns, and they emerged from a systematic review of 25 literature sources and directly shaped the operational structure of the proposed framework. The framework responds by extending three international standards, ISO 31000:2018, ISO/IEC 27701:2025 and ISO/IEC 29134:2023, with concrete fairness metrics and structured criteria to identify and reduce bias in automated decision-making [32,52]. Fairness issues in DPIAs, however, cannot be purely technical. It involves discretionary judgement and proportionality assessments, reflecting the broader role of DPIAs as fundamental rights governance instruments rather than compliance checklists [37,56]. Retaining "AI-driven Digitalisation" in the framing keeps IoT, Blockchain, and Big Data Analytics within scope, consistent with the four-technology focus maintained throughout the paper.

The above results raise a number of issues worthy of further discussion. Firstly, the use of algorithms in modern data processing techniques and data-intensive technological trends suggests the adoption of a broader view of DPIA is now appropriate and necessary to include consideration of AI, blockchain, IoT, data analytics and other digital technologies. This challenge is reflected in the regulatory landscape, as the EU AI Act introduces a separate category of high-risk AI systems for certain AI applications and may require a FRIA that complements the DPIA mandated under Article 35 GDPR. From a legal perspective, determining whether a particular technology meets privacy and data protection requirements prior to its implementation may have proved problematic for researchers, particularly in terms of the technical aspects of DPIA implementation. Privacy and data protection issues may also have contributed to the relatively limited number of studies regarding technology-focused DPIA, given that both the technologies themselves and their regulatory environments are rapidly evolving. There is a growing need to expand the scope of DPIAs to address the impacts of digitalisation and evolving privacy requirements. This expansion is critical as organisations increasingly adopt digital technologies which introduce new dimensions of privacy risks that traditional DPIA methodologies may not adequately cover. The EU AI Act reflects the growing recognition that DPIAs alone may not address the

broader implications of digitalisation on human rights, signalling a shift towards integrated assessment models combining data protection and fundamental rights perspectives. Analyses by Rintamäki et al. [9] further indicate that overlaps between GDPR DPIA obligations and AI Act FRIA requirements may create additional compliance complexity and inconsistencies in the assessment of high-risk AI systems across jurisdictions.

Secondly, DPIAs should now be viewed as an integral part of modern data protection strategies, particularly in the regulatory landscape shaped by GDPR. As technological advances drive the proliferation of data-driven processes, organisations face significant challenges in effectively implementing DPIAs. These challenges are multifaceted and encompass complex legal and regulatory frameworks, intricate risk assessment processes, and the inherent complexity of implementing DPIA. In this context, the framework put forward here provides an approach to addressing the challenges organisations face in DPIA implementation. It represents a conceptual shift by positioning DPIAs as a continuous governance mechanism rather than a one-time compliance activity. The internalisation of the PDCA cycle within the framework ensures that risk assessment, mitigation measures and accountability processes are revisited and refined in light of evolving technologies, changing data environments and emerging regulatory guidance. This iterative structure is particularly valuable in the context of AI, big data analytics, and IoT, where potential privacy risks cannot be fully identified at the outset and may only materialise after deployment. By integrating planning, implementation, verification, and adaptation into the DPIA process, the framework enables organisations to operationalise core GDPR principles, particularly transparency, fairness, and accountability, while ensuring long-term alignment between business objectives, technical feasibility, and fundamental rights protection. This approach strengthens the robustness of DPIAs and highlights the need for adaptive, reflexive methodologies that evolve alongside new technological developments. Whilst the construct validity of the framework is supported by the convergence of three independent structural sources (Table 6), its predictive and operational validity in organisational settings remains to be tested through case study or action research; this is addressed in the limitations and future research.

Thirdly, the findings of this review point to the emergence of a governance gap between DPIA obligation and organisational capability. Whilst the GDPR mandates the conduct of DPIAs for high-risk processing activities, it provides limited prescriptive guidance on the methodological rigour required to satisfy this obligation. This reflects a structural policy-implementation gap: the GDPR, as a principles-based regulatory policy instrument, deliberately establishes the obligation to conduct DPIAs without specifying implementation methodology, leaving this to supervisory authority guidance and organisational discretion. However, the policy implementation mechanisms intended to close this gap—supervisory authority guidelines, national adaptations, and sectoral guidance—remain fragmented and inconsistently applied across jurisdictions, which perpetuates interpretive variability and undermines the coherence of DPIA governance at the organisational level. As Georgiadis and Poels [3] and Moniz [37] both observe, this results in significant variability in DPIA quality, depth and consistency across organisations and jurisdictions.

Recent studies further indicate that DPIA implementation practices across organisations remain insufficiently standardised, particularly regarding methodological approaches, workflow structures and multi-stakeholder assessment processes [13,37]. The framework proposed in this study begins to address this gap by offering a structured, repeatable methodology grounded in the PDCA cycle; however, the effective deployment of this framework requires organisational investment in privacy competence, cross-functional governance structures, and tooling support. In this regard, there is a pressing need for supervisory authorities and standards bodies to develop more operationalised guidance—for

instance, sector-specific DPIA templates, auditable metrics for risk assessment quality, and certification schemes for DPIA practitioners—that would reduce interpretive variability and strengthen accountability. This is particularly relevant for small and medium-sized enterprises, which may lack the resources to navigate the methodological complexity of DPIA implementation without structured guidance.

The framework is intended as a comprehensive governance reference model rather than a prescriptive checklist that requires full sequential execution in every DPIA context. Its four-level hierarchy is explicitly designed to support modular adoption: organisations may enter the framework at the Risk Management Domain level and select only those Control Objectives and Operational Activities that are relevant to their specific processing context, technology environment, and organisational maturity. Smaller organisations or teams with limited privacy expertise are not expected to implement all domains simultaneously; rather, the framework provides a structured reference against which they can identify current capability gaps and prioritise implementation effort accordingly. The modular re-assessment capability, whereby practitioners can selectively re-execute only the Lifecycle Phases and Risk Management Domains affected by a significant change, further reduces the implementation burden in resource-constrained environments. Implementation burden is therefore acknowledged as a real operational constraint. The framework's full scope is intended for mature DPIA governance environments; leaner, domain-selective adoptions are methodologically legitimate provided the scope decisions are documented and justified within the organisation's DPIA report.

A further analytical distinction concerns whether the identified challenges are specific to DPIA or symptomatic of broader organisational governance conditions. Several of the challenges synthesised in Phase 1 are not unique to DPIA practice. The need for multidisciplinary expertise (C9), the time-consuming nature of cross-functional collaboration (C10), and the integration of technical and legal understanding (C4) are conditions that affect many compliance and risk management processes, including information security management, internal audit, and broader regulatory compliance. These may be more accurately characterised as general governance challenges that manifest within DPIA rather than DPIA-specific obstacles. By contrast, challenges such as the divergence of GDPR risk from traditional risk management (R1), the requirement to assess risk from the data subject's perspective rather than the organisation's (R5), the operationalisation of the GDPR fairness principle within impact assessment (C6), and the lack of a legal obligation for AI-based business models (L1) are intrinsic to the DPIA instrument and its specific regulatory foundation. Recognising this distinction has practical implications: DPIA-specific challenges require methodological and instrument-level solutions of the kind the proposed framework offers, whereas general governance challenges require organisation-wide structural responses such as cross-functional governance bodies, clear accountability allocation, and sustained investment in privacy competence. The proposed framework addresses the former directly and supports the latter indirectly, by embedding DPIA activities within a governance structure that makes cross-functional coordination and accountability explicit. It does not, however, substitute for the broader organisational governance maturity on which effective DPIA implementation ultimately depends.

Fourthly, the framework's grounding in three complementary international standards—ISO 31000:2018 for the risk management process backbone, ISO/IEC 27701:2025 for privacy management system requirements, and ISO/IEC 29134:2023 for the privacy impact assessment process—reflects a deliberate methodological choice. The Risk Management Domain structure of the framework derives its phase decomposition from ISO 31000 §6 (Scope, Context and Criteria; Risk Assessment; Risk Treatment; Monitoring and Review; Recording and Reporting; Communication and Consulta-

tion), while its privacy-specific Control Objectives derive from the Annex A controls of ISO/IEC 27701 and the process steps of ISO/IEC 29134. Where these privacy standards do not yet provide explicit guidance—particularly in relation to algorithmic fairness, broader socio-ethical impact, and adaptation to emerging technologies—the framework extends them in alignment with the EU AI Act Article 27 Fundamental Rights Impact Assessment requirement. The framework also remains compatible with the broader information security ecosystem through the ISO/IEC 27001:2022 [58] baseline that underpins the Cybersecurity Integration operational activity. This grounding addresses one of the key challenges identified in Phase 1—namely R1, that GDPR risk differs from traditional risk management—by providing a structured mechanism through which privacy risk can be operationalised without being subsumed under, or detached from, the organisation's broader risk management and information security practices. This is particularly relevant for organisations that already operate ISO/IEC 27001:2022-certified ISMS environments and need to integrate DPIA practices without duplicating governance structures.

Fifthly, the proposed framework makes the PDCA cycle operationally explicit at the activity level, whereas in the three reference standards the PDCA logic remains structurally embedded but not operationally explicit. ISO/IEC 27701:2025 is itself a management system standard structured according to the High-Level Structure introduced by ISO Annex SL, and its clauses on Planning (§6), Operation (§8), Performance Evaluation (§9) and Improvement (§10) implement the PDCA logic; ISO/IEC 29134:2023 follows a comparable iterative flow from threshold analysis through preparation, performance and follow-up; and ISO 31000:2018 structures the risk management process as a continuous loop with communication and consultation as a continuous activity. By assigning each DPIA activity to a specific PDCA phase and Risk Management Domain, and by linking each activity to the literature- identified challenges it addresses, the framework provides a translation from structural to operational PDCA. This translation enables practitioners to perform targeted re-assessment when changes occur in the underlying processing activity: rather than re-conducting the entire DPIA process when a significant change occurs (as required by ISO/IEC 29134 §6.5.5 but not operationally specified), practitioners can identify which Lifecycle Phases and Risk Management Domains are affected by the change and re-execute those modules selectively, while preserving the audit trail of unaffected activities. This modular re-assessment capability is particularly relevant in environments where digital technologies evolve faster than the standards can be revised.

Sixthly, the findings indicate that fragmented and silo-based assessment approaches are increasingly insufficient for addressing the multidimensional risks posed by digital technologies and AI-driven systems. Recent studies emphasise that privacy and security risks are becoming increasingly interconnected, particularly in AI-driven and data-intensive environments [35], while broader ethical and fundamental rights implications have expanded the scope of traditional privacy-focused assessments [36,41]. Earlier compliance-oriented PIA literature had also emphasised the need to address legal, technical, organisational, and security-related aspects together within data protection compliance processes. In particular, AI-driven systems may simultaneously trigger DPIAs, FRIAs, cybersecurity assessments, and broader governance obligations, potentially resulting in fragmented assessment practices, duplicated efforts, and inconsistent risk treatment across organisations. Prior research has highlighted the growing convergence between privacy, security, and broader societal impact assessments, especially in the context of AI and data-intensive technologies [35,41]. In this regard, the proposed framework contributes by providing a unified operational structure that integrates legal, technical, organisational, and socio-ethical dimensions within a single PDCA-based lifecycle. This integrated approach also

aligns with the iterative, continuously improving, governance-oriented risk management principles emphasised in ISO 31000:2018 and ISO/IEC 27701:2025.

Finally, the findings suggest that the effectiveness of DPIA implementation depends not only on methodological structure, but also on organisational governance maturity and cross-functional collaboration. As both Georgiadis and Poels [3] and Moniz [37] observe, organisations often struggle to operationalise DPIA processes due to limitations in institutional privacy capability, interdisciplinary coordination and practical implementation capacity. In practice, effective DPIA implementation requires the coordinated involvement of legal, technical, cybersecurity, compliance and operational stakeholders, rather than responsibility being isolated within a single organisational function. This governance-oriented perspective is also reflected in ISO/IEC 27701:2025, which emphasises leadership commitment, organisational roles and responsibilities, competence, communication and continual improvement as core components of privacy information management systems. In this regard, the proposed framework supports a more integrated and collaborative governance structure, facilitating ongoing coordination between organisational functions throughout the DPIA lifecycle.

DPIA concerns meaningful organisational decision-making and not only standard alignment, and this consideration informed the selection of three reference standards. ISO 31000:2018, ISO/IEC 27701:2025, and ISO/IEC 29134:2023 are not compliance checklists; they are governance, risk, and control (GRC) instruments developed to support structured organisational decision-making. ISO 31000 is itself a risk management decision framework whose process steps, namely establishing risk criteria, risk evaluation, and risk treatment, require contextual judgement and prioritisation rather than mechanical conformance. ISO/IEC 27701:2025 follows the management system High-Level Structure, embedding leadership commitment, organisational roles, and continual improvement as governance functions directly concerned with decision-making. The framework therefore inherits the governance and risk dimensions of these standards, not merely their compliance dimension, and operationalises them at the activity level.

Beyond its compliance function, the framework is explicitly designed to support meaningful organisational decision-making, including the prioritisation of assessment activities, the exercise of proportionality judgments, and the contextual calibration of risk treatment. At the Risk Policy domain level, the ISO 31000-grounded methodology requires organisations to establish context-specific risk criteria before conducting risk analysis, ensuring that the subsequent assessment is calibrated to the organisation's specific processing context, data subjects, and technology environment rather than applied mechanically across cases. The framework also supports risk-based prioritisation: by requiring organisations to establish risk criteria at the outset, it enables them to rank processing activities by severity and likelihood and to allocate assessment effort proportionately, concentrating the most resource-intensive Operational Activities on the highest-risk processing rather than applying uniform depth across all cases.

At the Risk Analysis domain level, the CLIFOD-based contextual integrity approach requires practitioners to evaluate privacy risks relative to the specific social and informational norms governing each processing context, supporting judgement-based rather than purely metric-based risk identification. At the Fairness Assessment and Fairness Validation domains, the framework acknowledges, following Moniz [37], that fairness determinations and proportionality assessments within DPIAs are inherently discretionary: no algorithmic rule or standard-defined procedure can substitute for the data controller's contextual judgement about whether a processing activity is fair, necessary, and proportionate to its purpose. The framework therefore does not attempt to eliminate discretion from the DPIA process; it provides a structured scaffold within which discretion can be exercised

transparently, documented consistently, and reviewed iteratively across PDCA cycles. In this regard, the framework's compliance orientation and its support for practical judgement are complementary rather than competing properties: the standard alignment provides the accountability structure within which proportionality decisions are made and recorded, while the four-level hierarchy ensures that those decisions remain traceable to empirically identified challenges and verifiable by supervisory authorities or certification bodies.

The transferability of the challenge taxonomy to non-EU jurisdictions warrants explicit consideration. The four categories differ materially in their cross-jurisdictional applicability. Legal and regulatory challenges (L1–L3) are the most jurisdiction-specific, being grounded in GDPR Article 35 obligations, EU AI Act Fundamental Rights Impact Assessment (FRIA) requirements, and EU supervisory authority structures; their application in non-EU contexts would require adaptation to the applicable legal triggers and regulatory framework. Risk assessment challenges (R1–R7) address the methodology of privacy risk identification and exhibit moderate-to-high transferability, as the substantive problem of assessing risks to data subjects from automated processing is common across data protection regimes regardless of their specific legal basis. Implementation complexity challenges (C1–C15) are organisational and process-oriented and exhibit the highest transferability: interdisciplinary coordination requirements, tooling gaps, and multi-stakeholder assessment challenges are not GDPR-specific but reflect systemic implementation conditions in any regulated data processing environment. Scope enhancement challenges (S1–S5) are technology-driven and similarly transferable, as AI, IoT, big data, and biometric processing pose comparable DPIA scope challenges across jurisdictions. Researchers and practitioners in non-EU contexts may therefore apply the R, C, and S categories directly, and adapt the L category to their applicable regulatory framework.

5. Conclusions

In conclusion, the findings of this review provide a valuable roadmap for future research and practice in the area of DPIAs. By adopting the proposed comprehensive framework, organisations can gain a thorough understanding of the complexities of data protection, comply with the GDPR and other relevant regulations, and contribute to the broader goal of protecting individuals' privacy in the digital age. The proposed DPIA Framework integrates technical, legal, and socio-ethical dimensions to provide a holistic approach to risk assessment. It emphasises the inclusion of fairness metrics, continuous monitoring, and adaptation to ensure that DPIAs comply not only with legal standards but also uphold ethical principles. An illustrative PDCA-cycle walkthrough demonstrating the framework's application in an AI employment screening context is provided in Appendix C.

The contribution of this work lies in the synthesis and structuring of existing knowledge rather than in empirical novelty. The framework should therefore be understood as a strong conceptual and normative proposal: it offers a theoretically grounded, standards-aligned, and traceable structure for DPIA practice, while its effectiveness in real organisational settings remains to be established through subsequent empirical evaluation.

The proposed framework offers four concrete advantages over a direct application of ISO 31000:2018, ISO/IEC 27701:2025 or ISO/IEC 29134:2023 in technology-driven DPIA contexts. First, it organises the DPIA process around an explicit four-level hierarchy of Lifecycle Phase, Risk Management Domain, Control Objective and Operational Activity, providing organisationally actionable structure that the standards, by their generality, do not. Second, it explicitly traces each operational activity to one or more empirically identified DPIA challenges (challenge codes L, R, C, S in Figure 4), thereby converting the abstract requirements of the standards into a structure that responds to documented practitioner barriers. Third, it makes the PDCA cycle operationally explicit at the activity

level, rather than leaving it implicit at the management system or process level as the standards do, thereby enabling targeted re-assessment when significant technological or processing changes occur—an important capability when digital technologies evolve faster than the standards can be revised. Fourth, it integrates considerations that the standards do not yet explicitly address—algorithmic fairness, broader socio-ethical impact, and adaptation to emerging technologies—in alignment with the EU AI Act Article 27 Fundamental Rights Impact Assessment requirement. Appendix B Table A4 documents the clause-level mapping of each operational activity to all three standards, providing the audit trail that organisations need to demonstrate alignment to internal stakeholders, supervisory authorities and certification bodies.

The research has its limitations. The systematic literature review was confined to English-language peer-reviewed articles and conference proceedings published from 2018 onwards, and the inclusion criteria excluded non-EU-focused studies, which may limit the generalisability of the findings to other regulatory contexts. The restriction to English-language sources may have excluded relevant contributions in German, French, Dutch, and other European languages, where DPIA practice has been examined within distinct national supervisory authority frameworks. While the EU focus is methodologically consistent with the regulatory scope of the study—the GDPR, the EU AI Act, and the three reference ISO standards constitute the primary normative anchors of the proposed framework—it is acknowledged that DPIA-equivalent practices in non-EU jurisdictions such as the United Kingdom post-Brexit, Switzerland, Brazil under the LGPD, and South Korea under the PIPA may offer comparative insights into implementation challenges that are not captured in the present review. Furthermore, although sectoral exclusions were applied on the grounds of transferability rather than sectorality, the exclusion of certain highly regulated domains such as financial services may have limited the breadth of the evidential base in contexts where AI-driven data processing is particularly intensive. Future research should extend the evidential base to include non-EU regulatory environments and a wider range of sectoral contexts, which may reveal both jurisdiction-specific and cross-jurisdictional implementation challenges that strengthen or refine the proposed framework.

The proposed framework has not yet been empirically validated in an organisational setting and future research should therefore test the framework's applicability through case studies or action research in organisations operating across different sectors and technology environments. The framework also does not currently prescribe specific tooling or automation support for each phase, which represents an area for further development. In addition, the four-category taxonomy reflects the challenges evident in the 25 reviewed studies and should not be interpreted as a complete enumeration of all possible DPIA implementation challenges; further challenges may emerge from broader evidential bases, additional jurisdictions, and sectoral contexts not covered by the present review. Furthermore, formal inter-rater reliability statistics were not reported for the screening and coding phases, which may limit confidence in the thematic synthesis. The exclusion of grey literature from national data protection authorities—including guidance documents from the EDPB, CNIL, ICO, and comparable bodies—may have limited the practical coverage of the challenge taxonomy. Future reviews should consider integrating DPIA guidance documents alongside the peer-reviewed literature to capture implementation knowledge that does not appear in academic publication channels.

The continued development of DPIA methodologies will be critical to meeting the dynamic challenges posed by digitalisation and ensuring effective data protection. As technology continues to evolve, it is imperative that DPIA frameworks are continuously monitored, updated, and improved to remain effective and relevant. The inconsistency of existing PIA/DPIA methodologies and their lack of adaptation to technological processes pose significant challenges for organisations. The development of a harmonised DPIA framework, as advocated in this article, is necessary to provide clear and applicable guidance to organisations across sectors and geographies.

The results of this study will be of interest to a number of stakeholders. Organisations incorporating technological advances into their business processes can gain insight into a conceivable range of challenges that DPIA implementation may entail. This framework addresses the unique risks posed by digital technologies, incorporating fairness metrics, continuous monitoring, and adaptation to ensure compliance with legal standards and uphold ethical principles. Risk assessment is an important component of this comprehensive framework, and, in particular, the APSIA methodology, which integrates privacy and security assessments to provide a comprehensive approach to risk management, is included to enhance risk assessment processes. In addition, the framework emphasises the importance of contextual analysis in understanding the specific technological environment and identifying the specific risks posed by new technologies. This includes assessing data quality and sources, integrating cybersecurity measures to enhance overall data protection, and aligning data processing activities with both business objectives and data protection principles.

Author Contributions: Conceptualization, B.M. and N.E.Y.; methodology, B.M., N.E.Y. and M.W.; validation, B.M., N.E.Y. and M.W.; formal analysis, B.M. and N.E.Y.; investigation, B.M. and N.E.Y.; resources, B.M. and N.E.Y.; data curation, B.M., N.E.Y. and M.W.; writing—original draft preparation, B.M., N.E.Y. and M.W.; writing—review and editing, B.M., N.E.Y. and M.W.; visualisation, B.M. and N.E.Y.; supervision, B.M.; project administration, B.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All data used in this study are available from the cited sources.

Acknowledgments: This study is conducted within the scope of the EU Horizon WEM Cyber (Widening Excellence and Mentoring in Cybersecurity) Project (No. 101216854).

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Definitions and Summary of Included Studies

Table A1. DPIA/PIA definitions.

Data Protection Authority/Organisation	Definition	Reference
	DPIA	
Irish Data Protection Commission	"DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR."	Irish Data Protection Commission [59]

Table A1. *Cont.*

Data Protection Authority/Organisation	Definition	Reference
Information Commissioner's Office	"A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations."	Information Commissioner's Office [60]
Article 29 Data Protection Working Party	"A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them."	Article 29 Data Protection Working Party [12]
National Commission on Informatics and Liberty (CNIL)	"The Data Protection Impact Assessment (DPIA) is an approach that allows to map and assess the risks of a personal data processing and to establish an action plan to reduce them to an acceptable level."	National Commission on Informatics and Liberty [61]
Personal Data Protection Commission Singapore	"A DPIA involves identifying, assessing and addressing personal data protection risks based on the organisation's functions, needs and processes."	Personal Data Protection Commission Singapore [62]
	PIA	
Office of the Privacy Commissioner of Canada	"A PIA is a risk management process that helps institutions ensure they meet legislative requirements and identify the impacts their programs and activities will have on individuals' privacy."	Office of the Privacy Commissioner of Canada [63]
International Organization for Standardization	"PIA is an instrument for: — assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information (PII). — taking necessary actions, in consultation with stakeholders, to treat privacy risk."	ISO/IEC 29134 [23]

Table A2. Summary of Included Studies.

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
1. DPIAs' Role in Fundamental Rights Governance	Moniz [37]	The study examines how DPIAs under the GDPR function as both accountability tools and decentralised governance frameworks, positioning data controllers as quasi-judicial actors who adjudicate conflicts between fundamental rights. This article aims to explain the balancing and proportionality assessments embedded in DPIAs, identify structural challenges such as subjectivity, legitimacy and inconsistency, and propose reforms to strengthen the role of DPIAs in protecting fundamental rights in the digital age.	EU	Regulatory Compliance	AI	Conceptual
2. Establishing a comprehensive data protection impact assessment methodology for big data analytics in compliance with the GDPR	Georgiadis and Poels [40]	The study aims to enhance DPIA practices for big data analytics by validating nine Privacy Touch Points (PTPs) that are specific to risks arising from big data analytics processes. It also seeks to identify gaps in existing GDPR-aligned DPIA frameworks and propose methodological improvements. The study further aims to operationalize these PTPs, validated through Delphi rounds and expert interviews, into a refined DPIA framework tailored to environments where big data analytics is used. This improved framework is intended to address issues such as unclear controllership, re-identification risks, concerns of discrimination, transparency gaps and challenges related to stakeholder involvement.	EU	IT and Regulatory Compliance	Big Data Analytics	Mixed Method

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
3. Navigating data governance risks: Facial recognition in law enforcement under EU legislation	Gültekin-Várkonyi [43]	The study examines how the use of facial recognition technologies by law enforcement agencies creates four major data governance risks under the GDPR and the AI Act: data minimization, purpose limitation, data/system accuracy, and administrative challenges. The article aims to analyse these risks from legal, technical and practical angles, and proposes expanding the DPIA process and integrating it with the risk-management requirements of the AI Act to ensure that the deployment of facial recognition technologies for public security is more legitimate and respects privacy.	EU	Regulatory Compliance	Facial Recognition Technologies	Qualitative
4. Enhancing AI fairness through impact assessment in the European Union: a legal and computer science perspective	Calvi and Kotzinos [32]	To explore the potential of algorithmic impact assessments (AIA), including DPIA, to protect individuals from algorithmic harms. It examines the societal impact of AI systems and explores how AIA processes can integrate legal, social and computer science perspectives to enhance accountability, promote fairness and contribute to the development of fairer AI solutions within existing and future regulatory frameworks.	EU	IT	AI	Mixed Method
5. TRUSTEE's Framework for DPIAs: Safeguarding personal information in the Digital Era	Grammatopoulos at al. [30]	The research article aims to introduce and explore the TRUSTEE framework's holistic approach to GDPR-compliant DPIAs, emphasising the comprehensive assessment of data processing activities and the integration of technical, user-centric, ethical, social and legal perspectives. It also outlines the implementation process within the TRUSTEE framework, emphasising its commitment to improving data protection and providing stakeholders with a robust tool for protecting personal data in the digital age.	EU	Regulatory Compliance	Self-sovereign identity, Homomorphic encryption, Blockchain technology	Qualitative

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
6. Position Paper: The role of law in achieving privacy and security measures in smart buildings from the GDPR context	Leesakul and Morisset [34]	The symposium paper aims to explore the challenges of applying the GDPR in the context of smart buildings, focusing on the ambiguities surrounding personal data processing and data privacy management for building controllers. By identifying the key requirements for data controllers in managing data privacy in smart buildings, particularly through the conduct of DPIAs, the study seeks to address compliance issues and strike a balance between privacy protection and the benefits of smart building technologies. The article emphasises the need for empirical and interdisciplinary research to effectively address the compliance challenges posed by smart environments.	EU	Industrial Sector	Smart building technologies (sensors, IoT, pervasive computing)	Conceptual
7. The Processing goes far beyond "the app"—Privacy issues of decentralised Digital Contact Tracing using the example of the German Corona-Warn-App	Rehak and Kuhne [33]	The research article aims to assess the data protection implications of contact tracing apps in response to the COVID-19 pandemic in Europe, focusing on the requirements of the GDPR and the necessity of conducting DPIAs. By utilising the Standard Data Protection Model, the study identifies weaknesses and risks in current implementations, highlighting the need for enhanced data subject rights protection and proposing solutions to address these shortcomings.	Germany	IT and Healthcare	Contact tracing	Conceptual
8. Gender, data protection and the smart city: Exploring the role of DPIA in achieving equality goals	Calvi [53]	The research article aims to explore the impact of data protection law, in particular the DPIA, on the development of smart cities in the European Union, focusing on its potential to address fundamental rights challenges and empower women from diverse backgrounds. By exploring how data protection measures can mitigate the dynamics of oppression of women in smart cities, the study aims to initiate a discussion on how to enhance inclusivity and address challenges in urban environments shaped by data processing.	EU	Regulatory compliance	Digital infrastructure, sensors, IoT devices, big data analytics, and cloud computing	Conceptual

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
9. 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	López et al. [39]	The research aims to propose the adaptation of the DPIA as a legal requirement to assess technology proposals, focusing on privacy by design principles, with a particular emphasis on identity management technologies. By addressing the challenges of digital identity management and emphasising the importance of considering both architectural and user aspects in technology development.	EU	IT	Digital Identity Management systems	Conceptual
10. Fairness and Data Protection Impact Assessments	Kasirzadeh and Clifford [52]	The research purpose of this article is to critically evaluate the effectiveness of conducting a DPIA through the lens of fairness metrics, highlighting the theoretical importance of fairness considerations in the DPIA process and examining their practical implementation based on guidance from data protection authorities. The paper aims to assess the operationalization of fairness metrics within DPIAs, considering technical challenges, the contextual nature of fairness, and the pivotal role of data controllers in determining fairness.	EU	IT and Regulatory Compliance	Machine Learning Systems	Conceptual
11. Designing a GDPR compliant blockchain-based IoV distributed information tracking system	Campanile et al. [38]	The research objective of this article is to propose a reference model for a system that uses blockchain technology to create trustworthy data logging systems for the Internet of Vehicles, addressing privacy concerns and ensuring GDPR compliance in the European Union. The study aims to demonstrate how blockchain can support GDPR-compliant solutions for tracking the chain of responsibility in the event of accidents or damage related to vehicle maintenance, ultimately improving road safety and legal accountability. In addition, the article explores the role of DPIAs in ensuring that the implementation of blockchain technology in the Internet of Vehicles domain is in line with GDPR requirements and safeguards the privacy rights of individuals.	Italy	IT	Blockchain and the Internet of Vehicles (IoV)	Mixed Method

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
12. A Perfect Match: Converging and Automating Privacy and Security Impact Assessment On-the-Fly	Papamartzivanos et al. [35]	The research purpose of this article is to introduce the APSIA ("Automated Privacy and Security Impact Assessment") methodology, utilising interdependency graph models and data processing flows to assess privacy risks in Information and Communication Technology infrastructures. Through a case study in the assistive healthcare domain, the study demonstrates the efficacy of APSIA in quantifying privacy impacts and enhancing security and privacy assessments in heavily regulated sectors.	Greece and Denmark	IT and Healthcare	Information and Communication Technology infrastructure	Mixed Method
13. Evaluating privacy impact assessment methods: guidelines and best practice	Vemou and Karyda [47]	The research purpose of this article is to provide practical guidance for implementing PIA by proposing a PIA process that incorporates best practices from existing guidelines and privacy research. The paper critically reviews and assesses various PIA methods to identify best practices and support PIA practitioners, ultimately proposing a comprehensive PIA process and evaluation framework to enhance the support for PIA projects. This research aims to extend existing PIA guidelines by offering practical and comprehensive guidance to PIA practitioners, addressing gaps and providing practical support for organising and implementing PIA projects.	EU	IT	Information and Communication Technology systems	Qualitative

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
14. Data Protection Impact Assessment in Identity Control Management with a Focus on Biometrics	Bisztray et al. [42]	The research purpose of this conference paper is to evaluate the efficacy of two distinct privacy impact assessment frameworks within the realm of biometric data protection, specifically in the domain of identity and access control management (IAM). By leveraging insights from the SWAN project, which employs four biometric characteristics for authentication, the study aims to assess the capability of these frameworks in pinpointing sector-specific privacy risks associated with IAM and biometric identification. The comparative analysis conducted in this research seeks to provide insights into the practical utility of these frameworks in addressing privacy concerns related to the processing of biometric data in alignment with GDPR regulations.	EU	IT	Biometric Authentication and Identity Management Systems (IDMs)	Case Study
15. Privacy Regulations Challenges on Data-centric and IoT Systems: A Case Study for Smart Vehicles	Campanile et al. [50]	The research purpose of this conference paper is to address the security challenges faced by IoT systems, particularly focusing on privacy preservation in the context of sensitive user data and compliance with the GDPR. The study aims to investigate the potential of blockchain technology in enhancing the privacy and compliance of IoT systems with data protection regulations, as evidenced through a pilot study and DPIA focusing on the Internet of Vehicles (IoVs) case study.	EU	IT	IoT, Internet of Vehicles (IoV), and Blockchain Technology	Case Study
16. Ethical Considerations for Movement Mapping to Identify Disease Transmission Hotspots	Jong et al. [54]	The purpose of this paper is to explore the ethical considerations surrounding the use of mobility data, specifically mobile phone call detail records (CDRs), for mapping infectious disease transmission hotspots. The study aims to address the risks and benefits of using ICT data to track the movements of infected individuals and identify potential transmission hotspots, while also developing a model DPIA template for conducting similar assessments in the future.	EU	IT and Healthcare	Information and Communication Technology (ICT)	Qualitative

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
17. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment	Mantelero [41]	The research purpose of this article is to propose a new assessment model, the Human Rights, Ethical, and Social Impact Assessment (HRESIA), that integrates human rights, ethical considerations, and societal impacts into a comprehensive evaluation framework for data-intensive technologies, including DPIA. The aim is to address the limitations of existing assessment models and provide a broader perspective on the impact of data processing on fundamental rights and collective social and ethical values.	EU	IT	AI and Big Data	Conceptual
18. An Open-Source Software Tool to Facilitate Data Protection Impact Assessments	Riemann et al. [44]	The research purpose of this article is to introduce and evaluate the efficacy of the "DPIA click&go" tool, designed to simplify and streamline the DPIA process in medical research settings. The study aims to validate the tool's performance through a real-world project, comparing its capabilities with manually created DPIAs in terms of risk coverage and mitigation strategies, highlighting its potential to harmonise data protection practices at a larger, potentially European or global scale.	Germany	IT and Healthcare	IT infrastructure, Open-Source Software	Mixed Method
19. Practical fundamental rights impact assessments	Janssen et al. [36]	The research purpose of this article is to introduce a practical four-phased framework to assist organisations in performing DPIAs and fundamental rights impact assessments for their AI systems. This framework addresses the challenges of assessing risks related to fundamental rights and data protection, ensuring compliance with the GDPR, and mitigating potential infringements on fundamental rights in AI systems to maintain public trust and address societal consequences.	EU	IT and Regulatory Compliance	AI systems	Qualitative

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
20. Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review	Georgiadis and Poels [3]	The research purpose of this article is to conduct a systematic literature review to identify privacy, and data protection risks specific to the Big Data Analytics context, aiming to develop a comprehensive DPIA methodology. Through thematic analysis, the study defines nine Privacy Touch Points summarising identified risks, with the goal of assisting data processors and controllers in identifying, analysing, and mitigating privacy and data protection risks in the context of Big Data Analytics.	EU	IT	Big Data Analytics	Systematic Literature Review
21. A Semantic Specification for Data Protection Impact Assessments (DPIA)	Pandit [31]	The research purpose of this article is to address the challenges faced by stakeholders in conducting DPIAs under the GDPR by utilising linked-data to represent DPIA-related information in a consistent and reusable manner. The article introduces an extension to the Data Privacy Vocabulary (DPV) for documenting DPIAs and an ontology for risk management based on ISO 31000 standards, aiming to improve the management and sharing of DPIA information and pave the way for shared impact assessments in the context of emerging technologies like AI and Cybersecurity.	EU	IT	Semantic Web Technologies, AI	Conceptual
22. DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems	Henriksen-Bulmer et al., [29]	The research purpose of this article is to introduce the DPIA Data Wheel, a holistic privacy risk assessment framework based on Contextual Integrity, to assist practitioners in evaluating privacy risks associated with Cyber Physical Systems. The framework aims to enable comprehensive contextual inquiry into privacy risks, identify mitigation strategies, and facilitate GDPR compliance by assessing privacy concerns from both organisational and individual perspectives through empirical evaluation in real-world settings.	UK	IT	Cyber Physical Systems (CPS)	Mixed method

Table A2. *Cont.*

Title	Author(s)/ Year	Objective	Country/ Region	Sector Context	Technology Focus	Methodology
23. Impact assessment requirements in the GDPR vs. the AI Act: Overlaps, divergence, and implications	Rintamäki et al. [9]	The study examines the overlaps, divergences and practical implications between DPIA obligations under the GDPR and Fundamental Rights Impact Assessment (FRIA) obligations under the AI Act. The article aims to identify when high-risk AI systems involving personal data trigger overlapping assessment requirements across the GDPR and the AI Act, analyse the variance in DPIA requirements across EU and EEA jurisdictions, and propose a more harmonised and interoperable impact assessment approach to support information sharing and compliance throughout the AI value chain.	EU/EEA	Regulatory Compliance	AI systems and high-risk AI systems	Mixed Method
24. Illuminating the DPIA Blackbox—A Survey of Data Protection Impact Assessment Practices in Organisations	Hansen et al. [13]	The study investigates how DPIAs are implemented in organisational practice and examines the practical challenges, operational processes, and methodological approaches used by organisations when conducting DPIAs. The article aims to illuminate the "DPIA blackbox" by analysing how organisations operationalise DPIA activities, structure assessment practices, and address implementation-related decision-making in practice.	EU	Regulatory Compliance	N/A (process-oriented DPIA study)	Exploratory Qualitative Study
25. Regulating AI-Driven Triage: Fundamental Rights and Compliance Challenges in the European Union	Lazcoz et al. [51]	The study examines the legal and regulatory challenges associated with the use of AI-driven triage systems in emergency healthcare within the European Union. The article analyses the applicability of the AI Act, GDPR, and MDR to AI-supported emergency triage, focusing particularly on automated decision-making, human oversight, profiling, DPIAs, FRIAs, and patient rights in AI-assisted clinical decision-making.	EU	Healthcare/Regulatory Compliance	AI-driven triage systems, generative AI, large language models (LLMs), automated decision-making systems	Legal and Regulatory Analys

Appendix B. Derivation and Validation of the Proposed Framework

Table A3. Literature foundations of the proposed PDCA-based DPIA framework for AI-Driven Digitalisation.

Lifecycle Phase	Risk Management Domain	Control Objective	Operational Activity Details	Sources
PLAN Pre-Assessment Phase	Define Scope	Articulation of the data processing activities to be assessed	It is essential first to identify the need for a DPIA by considering whether the data processing activity is likely to result in a high risk to the rights and freedoms of individuals. This includes specifying the types of data processed, the purposes of the processing, the systems involved, and the geographical scope. In the context of big data analytics, for example, it is essential to understand how data from different sources is integrated and processed in order to effectively identify potential privacy risks. Detail the specific data types (e.g., personal identification information, behavioural data, transactional data), the objectives of processing (e.g., personalised marketing, service improvement, fraud detection), the technological systems used (e.g., databases, analytics platforms, cloud services), and the geographical regions where data processing occurs (e.g., EU, non-EU regions)	Information Commissioner' Office [64] Georgiadis and Poels [3] Wright and Her [45]
		Consideration of the specific technological context	Addressing the specific technological environment will help understand the unique challenges and risks associated with these technologies at a more pre-assessment stage, as it highlights the need to tailor the scope of the DPIA to the specific technological environment to ensure a comprehensive risk assessment at a later stage. For instance, AI systems may involve automated decision-making processes that need scrutiny for fairness and transparency. IoT devices may introduce additional risks related to data transmission and device security. Blockchain technologies, particularly in IoT systems, can present challenges related to data immutability and transparency. While blockchain can enhance compliance with privacy regulations by providing secure and tamper-resistant data management, it also raises issues such as the difficulty of modifying or deleting data to comply with GDPR's right to be forgotten.	Riemann et al. [44] Georgiadis and Poels [3] Mantelero [41] Bieker et al. [49] Campanile et al [38,50]
	Define Objectives	Aligning Data Processing with Business Goals	Ensure that the data processing activity supports the company's overarching goal of enhancing customer experience through personalised services. This involves integrating data protection principles into the organizational culture to ensure that privacy considerations are part of the decision-making process at all levels	Calvi and Kotzinos [32]
		Addressing Business Needs	Identify and document the specific business needs that the data processing activity is intended to meet, such as improving customer satisfaction, increasing sales through targeted marketing and optimising product recommendations. This ensures that data processing activities are fit for purpose and aligned with business objectives.	Grammatopoul et al. [30]
		Ensuring Data Minimization	Ensuring data minimization involves limiting the amount of personal data processed to what is strictly necessary for the purposes identified. This reduces the risk of unnecessary data exposure and enhances compliance with the principle of data minimization. In the context of Big Data Analytics, it is crucial to adopt data minimization strategies to mitigate the inherent privacy risks associated with processing large volumes of data from various sources. For instance, the importance of embedding data protection throughout the life cycle of data processing, particularly in environments with extensive data analytics operations, to prevent over-collection and misuse of personal data. In addition, the need to align data processing practices with data minimization principles to ensure that only the essential data required for specific purposes is processed, thereby reducing the likelihood of privacy breaches. Conducting data minimization during the Pre-Assessment Phase is essential because it allows organisations to identify and limit the scope of data collection from the outset, thereby setting a foundation for compliant data processing activities. This proactive approach ensures that data protection measures are integrated early in the data lifecycle, minimising risks and enhancing overall data governance.	Wright and Her [45] Georgiadis and Poels [3]
		Assessing Data Quality and Sources	Evaluate the quality and accessibility of the data to be used in the processing activity. Ensure that the data is accurate, complete, and reliable, and that it is sourced in a manner that complies with legal and ethical standards.	Papamartzivan et al. [35]
	Data Flow Mapping	Mapping the flow of data to understand how data is being collected, processed and shared	Implementing a detailed data flow mapping is crucial for identifying privacy and security risks effectively. This involves charting how data moves through different stages of collection, processing, storage, and sharing within the organisation. This process helps in pinpointing potential vulnerabilities and ensures comprehensive privacy risk assessments. The APSIA methodology (Papamartzivanos et al. [35]) emphasises the importance of detailed data flow mapping to identify privacy and security risks in ICT infrastructures. It incorporates the use of interdependency graphs to visualise visualize the relationships between data assets, processing activities, and associated vulnerabilities. This graphical representation supports the identification of risky data processing activities by highlighting the interconnections and dependencies between different assets, thus enabling a dynamic and thorough privacy risk assessment. In this regard, best practices for conducting privacy impact assessments include comprehensive data flow analysis to understand the data lifecycle and potential risk points. This involves creating detailed diagrams that map out every stage of data processing, from collection to deletion, and identifying the entities involved at each stage. Such thorough mapping helps organisations ensure compliance with GDPR and other regulatory requirements by providing a clear overview of data processing activities and their associated risks.	Papamartzivan et al. [35] Vemou and Karyda [47]

Table A3. *Cont.*

Lifecycle Phase	Risk Management Domain	Control Objective	Operational Activity Details	Sources
PLAN Pre-Assessment Phase	Stakeholder Engagement	Involving all relevant stakeholders, including legal, technical and ethical experts, as well as representatives of affected communities	This is critical to ensure that all perspectives are considered and that the DPIA addresses the full privacy and data protection needs of the organisation. Accordingly, evolving DPIA frameworks should adapt to the dynamic nature of technology and the increasing volume of data being processed. This approach ensures that the DPIA remains relevant and effective in mitigating the risks associated with new and emerging technologies. Stakeholder engagement should also involve people from different parts of the organisation to ensure strong buy-in and diverse expertise. In this regard, heterogeneous organisational practices and insufficiently assessed multi-stakeholder processes may further complicate the practical implementation of DPIAs. The literature review revealed that the importance of ongoing stakeholder engagement throughout the DPIA process and continuous interaction with relevant stakeholders ensures that data protection measures are in line with actual data processing activities and dynamic changes in the technological environment. This ongoing engagement is crucial to effectively identify and mitigate data protection risks, especially in complex environments such as smart cities and IoT systems. In addition, the involvement of stakeholders such as legal advisors, technical experts and community representatives helps to address different concerns and ensures that the DPIA is comprehensive. The inclusiveness of the DPIA process ensures that the expertise of different stakeholders is utilised to identify potential risks and develop effective mitigation strategies. This is particularly important in scenarios involving advanced technologies such as AI and IoT, where the expertise of technical stakeholders is essential for understanding and addressing specific risks. Lastly, involving stakeholders from different backgrounds ensures that the DPIA can address not only technical and legal aspects, but also social and ethical implications. In this regard, by engaging a wide range of stakeholders, organisations can ensure that the DPIA process is robust, inclusive and able to address the complex and evolving landscape of data protection.	Hansen et al. [1 Wright and Her [45] Grammatopoul et al. [30] Mantelero [41] Calvi [53]
PLAN Risk Identification and Impact Evaluation	Risk Policy	Developing a risk policy based on ISO 31000 risk management standard to systematically identify risks, mitigations, consequences, and impacts	ISO 31000 risk management standard provides principles and guidelines for risk management, emphasising the importance of establishing a structured framework to address risks in a consistent and effective manner. According to ISO 31000, risk management should be integrated, structured, comprehensive and appropriate to the context of the organisation. In this context, the literature review proposed an extension of the Data Privacy Vocabulary (“DPV”) (Pandit [31]) to document DPIA-related information using an ontology based on ISO 31000 standards to improve consistency and reusability. This approach enables better management and interoperability by representing DPIA-related information as linked data and facilitates the sharing and reuse of risk-related information. In addition, overlaps and divergences between GDPR DPIA requirements and AI Act FRIA obligations further demonstrate the need for more harmonised and interoperable risk assessment structures capable of supporting consistent information sharing across the AI value chain (Rintamäki et al. [9]). The DPV includes comprehensive taxonomies for describing personal data processing activities, risks and DPIA concepts, making it a versatile tool for different risk management applications. In this regard, Georgiadis and Poels [40] emphasise that incorporating Privacy Touch Points, a structured set of recurring privacy challenges identified through expert consensus, including lack of transparency, purpose expansion, inference-related risks and procedural ambiguity, into DPIA structures can strengthen methodological clarity and improve the consistency of risk-related decision-making in complex, technology-intensive environments. On the other hand, the review highlighted the need for structured risk assessments in AI systems in order to effectively manage risks to individual rights and freedoms. The need for a well-defined risk ontology that integrates legal, social and technical perspectives, provides a holistic understanding of the impact of AI, and promotes fairness and accountability was advocated. By combining these methodologies and adhering to the principles of ISO 31000, organisations can develop a robust risk ontology that supports comprehensive risk identification and management, improves the effectiveness of DPIAs and ensures compliance with data protection regulations.	Rintamäki et al. [9] ISO 31000 [28] Pandit [31] Calvi and Kotzinos [32] Georgiadis and Poels [40]

Table A3. *Cont.*

Lifecycle Phase	Risk Management Domain	Control Objective	Operational Activity Details	Sources
PLAN Risk Identification and Impact Evaluation	Risk Analysis	Conducting a comprehensive contextual analysis to identify potential privacy and security risks associated with data processing technologies, ensuring data protection through proactive assessment and mitigation strategies	A comprehensive identification of potential privacy risks, covering both physical and technological processes, is essential to ensure data protection. The literature has highlighted the complexity of risk assessment, emphasised the need for a comprehensive analysis of both physical and technological risks due to the integration of multiple sensors and systems, creating a socio-technical environment where privacy concerns must be carefully managed to prevent unauthorised access and data breaches, and advocated a DPIA that includes comprehensive assessments of data flow, storage and processing activities to address potential risks such as identity theft and unauthorized data access, underlining the importance of detailed risk identification and mitigation strategies. Accordingly, it is recognised that conducting a comprehensive contextual analysis is critical to understanding the specific technological environment and identifying potential privacy and security risks associated with data processing activities, including AI, big data, IoT and blockchain. The literature review discussed the CLIFOD framework (Henriksen-Bulmer et al. [29]), which integrates physical, human, and technological components to provide a comprehensive privacy risk assessment using Nissenbaum's Contextual Integrity (Nissenbaum [65]) which defines privacy as appropriate information flows within specific social contexts, based on key aspects including the context itself, the actors involved, the types of information being shared, and the transmission principles governing how information is exchanged. The stages of the framework, namely disclosure, risk assessment and decision making, enable organisations to systematically identify and mitigate privacy risks in cyber-physical systems. In addition, conducting a contextual risk analysis prior to commencing data processing activities is critical to identifying vulnerabilities specific to the technologies used. In AI-supported decision-making environments, this analysis should also consider automation bias, meaningful human oversight and workflow-integrated safeguards in order to effectively mitigate risks associated with high-risk AI systems (Lazcoz et al. [51]). This proactive approach ensures that potential privacy and security risks are fully understood and mitigated. By assessing the weaknesses and vulnerabilities of AI, big data, IoT and blockchain technologies in advance, organisations can implement appropriate protection and compliance measures, thereby improving overall data security and regulatory compliance. In this context, the review highlighted the importance of understanding the technological context of GDPR-compliant blockchain systems in the IoT to effectively address privacy risks. As highlighted in the UK government's research on cybersecurity risks to AI, which highlights the need for comprehensive assessments to mitigate potential risks, it is crucial to identify specific vulnerabilities of technologies prior to implementation.	Lazcoz et al. [51] UK-Governmer [66] Henriksen-Bulmer et al. [29 Campanile et al [38] Nissenbaum [65 Leesakul and Morisset [34] Bisztray et al. [4
	Fairness Assessment	Implementing fairness metrics to ensure that data processing activities are fair and equitable, integrating comprehensive frameworks and intersectional considerations to mitigate bias	The application of fairness metrics is crucial for assessing the impact of data processing activities on individuals' rights and freedoms, and for ensuring that these activities are carried out in a fair and equitable manner. The systematic literature review presented a framework for integrating fairness metrics into DPIAs, highlighting their importance for operationalizing the fairness principle in the GDPR and for systematically assessing and mitigating bias in data processing, particularly in AI systems. The framework includes a detailed review of the fairness principle in Article 5(1)(a) of the GDPR and its application to DPIAs, highlighting the need for concrete, quantified fairness metrics to bridge the gap between regulatory frameworks and AI systems. Specifically, the review discusses the role of fairness in data protection in smart cities, highlighting the need to assess the impact on different populations and consider cross-cutting aspects such as gender, race and socio-economic status to avoid disproportionate impacts on vulnerable groups. In this context, companies should apply fairness metrics as part of their DPIAs to ensure that data processing activities are fair and equitable. This includes integrating comprehensive frameworks and cross-cutting considerations to effectively mitigate bias. Furthermore, Moniz [37] highlights that fairness assessments within DPIAs inherently rely on discretionary balancing and proportionality judgments by data controllers, which introduces risks of subjectivity and inconsistency when determining whether processing is fair. This way, organisations can align their data processing practices with legal requirements and promote social justice by ensuring that their technology serves all populations in a fair and responsible manner.	Calvi [53] Kasirzadeh and Clifford [52] Moniz [37]
	Ethical Analysis	Conducting an ethical impact assessment to address socio-ethical implications and promote fairness	The literature review highlighted the importance of assessing the ethical implications of data protection, with a particular focus on inclusiveness and the needs of diverse populations and argued that it should consider how data processing affects different demographic groups and ensure that activities promote fairness and equality. It stressed the importance of integrating ethical considerations into the DPIA process, particularly in the context of AI and big data, and of addressing wider societal impacts and ensuring that data processing activities do not disproportionately affect vulnerable groups. Gültekin-Várkonyi [43] emphasises that technologies such as facial recognition and AI-driven surveillance create significant socio-ethical concerns, including mass surveillance risks, erosion of individual autonomy, unequal impacts arising from accuracy disparities and the normalisation of intrusive monitoring practices, and therefore argues that DPIAs should adopt a human-rights-oriented ethical analysis that explicitly evaluates these broader societal harms and fundamental-rights implications when assessing emerging data-intensive systems. Ethical Impact Assessments are necessary to maintain public trust and ensure that data processing activities are in line with societal values; therefore, companies should assess the potential socio-ethical impacts of data processing activities and integrate these ethical considerations into their DPIA processes in order to promote fairness, build public trust and align their practices with societal values. In order to conduct an effective Ethical Impact Assessment, companies should engage with diverse stakeholders, including representatives from different demographic groups and communities, to gather different perspectives on the potential impacts of data processing activities. They should systematically identify and assess potential harms and benefits, ensuring that vulnerable populations are considered. Ensuring transparency and accountability, by making the decision-making process transparent and holding those responsible accountable for their decisions, fosters trust and upholds ethical standards. In addition, companies should document and monitor their ethical considerations and assessments and continually monitor impacts to adapt and improve practices over time. By following these steps, companies can ensure that their data processing activities are fair, ethical and in line with societal values.	Calvi [53] Mantelero [41] Gültekin-Várkonyi [43]

Table A3. *Cont.*

Lifecycle Phase	Risk Management Domain	Control Objective	Operational Activity Details	Sources
PLAN Risk Identification and Impact Evaluation	User Rights Impact Analysis	Assessing how data processing activities impact the rights of data subjects, including the right to access, rectify, erase, and restrict processing of their data	Assessing how data processing activities affect the rights of data subjects, including their rights to access, rectification, erasure and restriction of the processing of their data, ensures compliance with GDPR requirements and promotes the protection of individual rights. The literature review advocated the importance of assessing privacy by design in identity management systems, emphasising both architectural and user aspects to address digital identity management challenges and adapt DPIA as a legal methodology. The need for comprehensive DPIA frameworks to effectively protect the rights of data subjects and the importance of fairness criteria in the DPIA process to ensure that data processing activities respect the rights and freedoms of individuals was emphasized, highlighting in particular the complexities of big data analytics. Regular review and updating of these procedures are crucial to address emerging challenges and maintain compliance. By implementing transparent procedures for data subjects to exercise their rights, providing regular GDPR training to employees, regularly reviewing and, where necessary, updating data protection policies, and using fairness criteria to ensure non-discriminatory data practices, organisations will not only comply with the GDPR and other relevant regulations, but will also improve the protection of data subjects' rights, build trust with their customers, and demonstrate their commitment to privacy, thereby increasing customer satisfaction and loyalty.	López et al. [39] Kasirzadeh and Clifford [52] Georgiadis and Poels [3]
	Technical Feasibility	Ensuring that proposed privacy measures are practical and can be effectively implemented	Discussing technical feasibility with subject matter experts is critical to assessing the feasibility of proposed safeguards. The literature review highlighted the importance of assessing the technical feasibility of identity management systems to ensure the practical implementation of privacy measures. This includes assessing the technical capabilities of the systems to support privacy-enhancing technologies such as encryption, anonymization, and secure access controls. It is also important to assess the ability of the system to integrate these technologies without compromising performance or user experience. It also highlights the need to assess the technical feasibility of blockchain-based IoT systems, focusing on the scalability, reliability and security of blockchain solutions in managing IoT data. This includes ensuring that blockchain technologies can maintain data integrity and confidentiality when processing the large volumes of data generated by IoT devices. Companies should conduct thorough technical assessments, including stress testing and performance evaluations, to identify potential technical limitations and opportunities for optimisation. Working with experts in relevant fields can help companies implement robust and effective privacy protections by providing valuable insight into the latest technological developments and best practices. By thoroughly assessing technical feasibility, organisations can ensure that privacy measures are not only theoretically sound, but also practically feasible, resulting in enhanced privacy and legal compliance. This proactive approach to assessing technical feasibility will help to create flexible data protection frameworks that can adapt to technological developments and changing threats.	López et al. [39] Campanile et al [50]
DO Mitigation Strategies	Technical and Organizational Measures (TOMs)	Ensuring comprehensive protection of personal data through effective technical and organisational measures	Implementing TOMs such as encryption, access controls and data minimisation and taking a holistic approach to TOMs and integrating them into the overall risk management framework to ensure robust data protection across the organisation is critical to protecting personal data and ensuring compliance with data protection regulations. The PACTS methodology of the TRUSTEE framework (Grammatopoulos et al. [30]) from the literature review emphasises a structured approach to risk management and outlines effective strategies for the development and implementation of risk mitigation measures. The Preparation component of the PACTS methodology involves identifying potential risks and preparing a comprehensive plan to address those risks; Assessment involves evaluating the identified risks and their potential impact on data protection; Control involves implementing measures to control and mitigate the identified risks and data protection; Monitoring involves tracking the effectiveness of implemented measures and monitoring changes in risk levels; and Sharing involves sharing information about risks and mitigation strategies with relevant stakeholders to ensure transparency and collaborative risk management. Companies should be encouraged to adopt this methodology to ensure a comprehensive and systematic approach to risk mitigation, technical guidelines, recognise the importance of integrating cybersecurity measures into privacy frameworks to enhance data protection, and conduct continuous monitoring and periodic reviews to maintain the effectiveness of implemented strategies. The need to ensure the precise definition and implementation of technical and organisational measures tailored to specific data protection needs was also highlighted in the studies.	Grammatopoul et al. [30] Pandit [31] European Union Agency for Network and Information Security [67]
	Cybersecurity Integration	Enhancing data protection by integrating cybersecurity measures with privacy frameworks	The literature review highlighted the APSIA methodology (Papamartzivanos et al. [35]), which integrates privacy and security assessments to provide a comprehensive approach to risk management. In particular, it highlighted the need to integrate cybersecurity into DPIAs in the context of big data analytics to address the unique security challenges posed by large-scale data processing. Accordingly, it highlights the importance of companies incorporating cybersecurity measures into their privacy frameworks to enhance data protection. By ensuring that cybersecurity practices are integrated into privacy frameworks to effectively address both security and privacy risks, organisations can enhance their overall risk management strategy, improve data protection compliance, and build customer trust by demonstrating a strong commitment to data security and privacy. This integration aligns the privacy framework with the Information Security Management System baseline specified in ISO/IEC 27001:2022, whose Annex A controls (organised under organisational, people, physical and technological themes) are explicitly referenced by ISO/IEC 27701:2025's Annex A.3 as the security controls underpinning a PIMS.	Papamartzivan et al. [35] Georgiadis and Poels [3] ISO/IEC27701: 2025 [14]

Table A3. *Cont.*

Lifecycle Phase	Risk Management Domain	Control Objective	Operational Activity Details	Sources
DO Documentation and Reporting	Comprehensive Documentation	Documenting all phases of the DPIA process, including identified risks, mitigation strategies, and stakeholder consultations	Documenting all stages of the DPIA process, including the pre-assessment phase, will ensure that every aspect of the DPIA is meticulously recorded and will provide a comprehensive and reusable reference. The literature review highlighted the importance of using an expanded data privacy vocabulary, which is an extended vocabulary designed to provide a structured and comprehensive framework for documenting data privacy activities, ensures that all aspects of data privacy are clearly defined and consistently documented, facilitating better communication, understanding, and management of privacy risks and compliance measures within an organisation, for detailed documentation and that all data privacy activities should be clearly defined and consistently documented. It also highlighted the need to document fairness criteria and impact assessments that provide a transparent record of how decisions were made and their potential impact on data subjects. This level of detail is critical to maintaining corporate accountability and due diligence in data protection practices.	Pandit [31] Kasirzadeh and Clifford [52]
	Transparent Reporting	Ensuring transparent reporting to stakeholders and regulatory authorities, clearly communicating how privacy risks are managed and mitigated	Transparent reporting includes regularly updating stakeholders on the results of the DPIA, including steps taken to address identified risks. In particular, the importance of conducting privacy impact assessments and transparently communicating the results to all relevant parties should be recognised. This should include detailed reports explaining the reasoning behind decisions and the effectiveness of the measures taken. The literature review recommends transparent reporting in big data DPIAs, emphasizing that findings should be communicated in a clear and comprehensive manner to maintain stakeholder trust and compliance. Companies should ensure that all DPIA activities are clearly and effectively communicated to stakeholders by establishing regular reporting protocols. This practice not only increases accountability but also builds trust and demonstrates a commitment to privacy. By implementing robust documentation and transparent reporting practices, organisations can ensure ongoing regulatory compliance and create a culture of data privacy transparency and accountability.	Georgiadis and Poels [3] Information Commissioner' Office [11]
CHECK Continuous Monitoring	Monitoring and Review	Maintaining the effectiveness and relevance of data protection measures through continuous monitoring and regular updates	Mechanisms for continuous monitoring and periodic review of privacy measures should be put in place to ensure continuous adaptation and adjustment to new risks. The literature review supports continuous monitoring as part of the CLIFOD framework (Henriksen-Bulmer et al. [29]) and highlights the importance of continuous assessment and adaptation of data protection measures. It also highlighted the need for regular updates and improvements to address emerging threats and evolving legal requirements. In this context, organisations should implement automated monitoring systems to monitor data processing activities in real time, enabling rapid detection and response to potential security incidents. Regular audits and assessments should be conducted to evaluate the effectiveness of existing data protection measures and identify areas for improvement. By establishing a feedback loop, organisations can ensure that their privacy policies evolve in line with technological developments and regulatory changes. It is also recommended that a dedicated team be established to oversee the ongoing monitoring and review process, ensuring accountability and a continued focus on privacy. Working with external auditors and industry experts can provide additional insight and verify the robustness of the measures in place. This proactive approach helps organisations take a strong data protection stance, ensure compliance and build trust with stakeholders.	Henriksen-Bulmer et al. [29] Vemou and Karyda [47]
CHECK Compliance Verification	Legal Compliance Check	Ensure compliance with GDPR and other relevant privacy legislation	The Article 29 Data Protection Working Party Guidelines (Article 29 Data Protection Working Party [12]) outline the requirements for assessing processing activities to ensure compliance with the principles of the GDPR. These and similar guidelines provide a structured approach to ensuring that data processing activities comply with legal standards, thereby protecting the privacy of individuals and supporting data protection legislation. Additionally, it is critical for organisations to comply with local data protection regulations, which may have specific requirements that go beyond the GDPR. In the literature review, the TRUSTEE framework (Grammatopoulos et al. [30]) highlights the importance of complying with local data protection laws to ensure comprehensive compliance. In addition, the Data Act provides a framework for managing data access and sharing in accordance with the law. Richter [68] argues that the Data Act aims to facilitate data sharing across sectors while providing robust data protection measures, and that compliance with the Data Act is crucial for organisations to balance innovation with the protection of fundamental rights and freedoms. Therefore, organisations should familiarise themselves with the provisions of the Data Act to understand the regulatory landscape for data access and sharing. This includes understanding the legal obligations for data protection and the measures required to comply with the Data Act and should ensure that they understand and implement the requirements of the Data Act to maintain legal compliance. Moreover, Moniz [37] argues that legal compliance checks within the DPIA should also evaluate the legitimacy of the underlying balancing and proportionality assessments, noting that mere adherence to regulatory provisions may be insufficient where fundamental rights are affected. By following these guidelines and ensuring comprehensive legal compliance by adhering to both the GDPR and local data protection regulations, organisations can not only avoid legal penalties but also enhance the organisation's reputation for data protection and build trust with stakeholders. Finally, seeking advice from privacy law experts can help navigate the complex regulatory landscape and ensure that all compliance measures are implemented effectively.	Grammatopoul et al. [30] Article 29 Data Protection Working Party [12] Richter [68] Moniz [37]

Table A3. *Cont.*

Lifecycle Phase	Risk Management Domain	Control Objective	Operational Activity Details	Sources
CHECK Compliance Verification	Fairness Validation	Verifying the fairness of data processing activities through the application of appropriate fairness metrics and transparency safeguards.	The validation of fairness requires assessing whether the data processing activity results in discriminatory effects, unequal outcomes, or systemic disadvantages for particular groups of data subjects, moving beyond formal compliance and examining the socio-technical implications of automated decision-making. In the context of emerging technologies such as AI and big data analytics, the DPIA should integrate concrete fairness metrics to systematically evaluate potential bias, ensuring that fairness is operationalised in line with the GDPR's fairness principle. Recent literature highlights that fairness within DPIAs must be based on measurable criteria rather than abstract normative interpretations and should be embedded in the risk assessment process by linking fairness metrics to mitigation strategies in AI-driven environments (Kasirzadeh & Clifford [52]), while acknowledging that fairness determinations ultimately depend on discretionary balancing and proportionality assessments that reflect the DPIA's nature as a fundamental rights governance instrument rather than a purely technical evaluation (Moniz [37]). The AI Act further reinforces this governance logic by embedding fairness evaluations into a continuous risk-based compliance framework for high-risk AI systems through mandatory data governance duties, bias mitigation obligations and post-market monitoring requirements. Accordingly, fairness validation requires identifying and justifying the fairness metrics applied, assessing their contextual adequacy, evaluating procedural safeguards such as transparency and documentation, and establishing mechanisms for continuous monitoring to address potential fairness-related harms over time. In this regard, fairness validation complements the overall compliance verification by ensuring that the processing activity not only satisfies legal requirements but also promotes equitable outcomes and accountability throughout the lifecycle of advanced data processing systems.	Kasirzadeh and Clifford [52] Calvi and Kotzinos [32] Georgiadis and Poels [40] Moniz [37]
ACT Review and Adaptation	Periodic Reviews	Regularly reviewing the DPIA framework to incorporate new insights and regulatory updates	Periodic reviews ensure that the DPIA framework remains up-to-date and effective. The literature review highlighted the importance of regularly updating DPIA methodologies to keep pace with technological developments and emerging risks, as well as the importance of periodic reviews to ensure that DPIAs continue to address current and evolving privacy concerns. In this regard, companies should establish regular review programmes and engage with regulatory updates to incorporate the latest changes and best practices into their DPIA processes.	Mantelero [41] Janssen et al. [3
	Emerging Technologies	Continuously adapting the DPIA framework to address new challenges and risks posed by emerging technologies	Adapting the DPIA framework to emerging technologies is critical for effective privacy risk management. The literature review recommended modifying DPIA methodologies for big data analytics to address the unique challenges posed by large-scale data processing and argued for the need to adapt DPIA approaches for blockchain and IoT systems, highlighting the need to ensure that the framework remains effective in managing privacy risks in evolving technological contexts. In this context, companies need to keep abreast of technological developments and work with experts to continuously update DPIA methodologies to ensure robust and up-to-date privacy measures.	Georgiadis and Poels [3] Campanile et al [50]

Table A4. Derivation of the proposed PDCA-based DPIA framework for AI-Driven Digitalisation from ISO 31000:2018, ISO/IEC 27701:2025 and ISO/IEC 29134:2023.

Lifecycle Phase (PDCA)	Risk Management Domain	Control Objective	Operational Activity (Figure 4) and Addressed Challenges	ISO 31000:2018 Alignment (Process Backbone)	ISO/IEC 27701:2025 Mapping	ISO/IEC 29134:2023 Mapping
PLAN—Pre-Assessment Phase (aligns with ISO 31000 §6.3 Scope, Context and Criteria)						
Plan	Pre-Assessment Phase	Define Scope—articulation of the data processing activities to be assessed	Identifies the need for a DPIA, specifying data types, processing purposes, systems and geographical scope. Addresses L1, L2	§6.3.2 Defining the scope (subject of the risk management activity)	§4.3 Determining the scope of the PIMS; §6.1.1 Actions to address risks; A.1.2.6 PIA mandatory trigger	§6.2 Threshold analysis; §6.3.3 Describe what is being assessed; §7.3.1 Process under evaluation
Plan	Pre-Assessment Phase	Define Scope—consideration of the specific technological context	Tailors DPIA scope to AI, IoT, blockchain, or big data environments. Addresses L3, L2	§6.3.3 External and internal context (technological environment)	§4.1 Understanding the organisation and its context	§6.3.3 System design information; §7.3.1.3 System design
Plan	Pre-Assessment Phase	Define Objectives—aligning data processing with business goals	Integrates data protection principles into organisational decision-making	§6.3.3 Internal context (objectives, strategies)	§4.1 Context; §4.2 Needs and expectations of interested parties	§6.3.1 Risk criteria reflect organisation's values, objectives, resources
Plan	Pre-Assessment Phase	Define Objectives—addressing business needs	Documents specific business needs for fitness for purpose	§6.3.4 Defining risk criteria (linked to objectives)	§4.4 PIMS scope; §5.1 Leadership and commitment	§6.3.2 Business case and allocated resources for the PIA
Plan	Pre-Assessment Phase	Define Objectives—ensuring data minimisation	Limits processing to what is strictly necessary; critical for big data. Addresses L3, S3	§6.3.4 Risk criteria (linked to data minimisation principle)	A.1.4.2 Limit collection; A.1.4.3 Limit processing; A.1.4.5 PII minimisation	§6.4.3 Privacy safeguarding requirements (data minimisation)
Plan	Pre-Assessment Phase	Define Objectives—assessing data quality and sources	Evaluates accuracy, completeness, reliability and lawful sourcing	§6.3.3 External context (data sources)	A.1.4.4 Accuracy and quality of PII	§6.4.1 Identify information flows of PII (sources)
Plan	Pre-Assessment Phase	Data Flow Mapping	Charts data movement (collection, processing, storage, sharing) using APSIA interdependency graphs (Papamartzivanos et al. [35]). Addresses R4, C3, C7	§6.3.2 Defining the scope (boundaries and interfaces); §6.4.2 Risk identification (sources and events)	A.1.2.9 Records related to processing PII; A.3.5 Classification of information	§6.4.1 Identify information flows of PII; §7.3.1.2 System requirement information
Plan	Pre-Assessment Phase	Stakeholder Engagement (Stakeholder Management—see notes)	Multidisciplinary engagement throughout the DPIA. Operationalises ISO 31000 §6.2 Communication and Consultation as a continuous activity, framed as Stakeholder Management within the framework. Addresses L1, C9, C10, S1	§6.2 Communication and consultation (continuous, spanning all phases)	§4.2 Understanding needs and expectations of interested parties; §7.4 Communication	§6.3.4 Identify stakeholders; §6.3.5 Establish a consultation plan; §6.3.6 Consult with stakeholders
PLAN—Risk Identification and Impact Evaluation (aligns with ISO 31000 §6.4 Risk Assessment)						
Plan	Risk Identification and Impact Evaluation	Risk Policy—based on ISO 31000 to systematically identify risks, mitigations, consequences, and impacts	Establishes structured, repeatable risk methodology integrating PTPs (Georgiadis & Poels [40]) and DPV ontology (Pandit [31]). Addresses R1, R6	§5.4.2 Establishing a risk management policy; §6.1 General; §6.4.1 General	§5.2 Policy; §6.1.2 Risk assessment (built on ISO 31000); §6.1.3 Risk treatment	§6.3.1 Set up PIA team and provide direction (ISO 31000-based criteria)
Plan	Risk Identification and Impact Evaluation	Risk Analysis	Applies CLIFOD framework (Henriksen-Bulmer et al. [29]) based on Contextual Integrity. Addresses R1, R3, R4, R5, R7, C3	§6.4.2 Risk identification; §6.4.3 Risk analysis (likelihood and consequences)	§6.1.2 Risk assessment process (criteria, identification, analysis, evaluation); A.5.7 Threat intelligence	§6.4.4 Privacy risk analysis; §6.4.5 Privacy risk evaluation; Annex A scale criteria; Annex B Generic threats
Plan	Risk Identification and Impact Evaluation	Fairness Assessment	Operationalises GDPR Article 5(1)(a) fairness; complements EU AI Act Article 27 FRIA. Addresses C6, C8, S1, S3	Extends ISO 31000 §6.4.2 risk identification toward algorithmic bias as a non-traditional risk source	Partial—A.1.3.11 Automated decision-making addresses individual rights, not systemic fairness. Framework extends 27701 in line with AI Act	Partial—fairness not in §6.3.1 harm dimensions. Framework extends PIA toward algorithmic fairness assessment

Table A4. *Cont.*

Lifecycle Phase (PDCA)	Risk Management Domain	Control Objective	Operational Activity (Figure 4) and Addressed Challenges	ISO 31000:2018 Alignment (Process Backbone)	ISO/IEC 27701:2025 Mapping	ISO/IEC 29134:2023 Mapping
Plan	Risk Identification and Impact Evaluation	Ethical Analysis	Human-rights-oriented ethical analysis (Mantelero [41]; Gültekin-Várkonyi [43]) addressing surveillance, autonomy, vulnerable groups. Addresses C1, C6, S1, S2, S4	Extends ISO 31000 §6.4.3 consequences analysis toward socio-ethical impact	Not addressed—beyond 27701 privacy/security scope. Framework extension complementing AI Act FRIA	Not addressed—beyond 29134 PIA scope. Framework extension toward socio-ethical evaluation
Plan	Risk Identification and Impact Evaluation	User Rights Impact Analysis	Evaluates GDPR Articles 15-22 rights impact in identity management and big data contexts. Addresses R5, R6, C8	§6.4.3 Risk analysis (consequences for affected parties)	A.1.3.2 Obligations to PII principals; A.1.3.3–3.10 Rights of access, correction, erasure, objection	§6.4.3 Privacy safeguarding requirements; §7.3.2 Privacy requirements
Plan	Risk Identification and Impact Evaluation	Technical Feasibility	Assesses scalability, reliability, integration of privacy-enhancing technologies. Addresses C5	§6.4.4 Risk evaluation (informed by feasibility); §6.5.2 Selection of risk treatment options	§6.1.3 Risk treatment (selection of options); A.3.29 Secure system architecture	§6.4.6 Determine controls (consider feasibility); §6.4.7 Risk treatment plans
DO—Mitigation Strategies (aligns with ISO 31000 §6.5 Risk Treatment)						
Do	Mitigation Strategies	Technical and Organisational Measures (TOMs)	Implements TOMs through PACTS methodology of TRUSTEE framework (Grammatopoulos et al. [30]). Addresses C12, C13	§6.5.2 Selection of risk treatment options; §6.5.3 Preparing and implementing risk treatment plans	A.1.4.6 De-identification; A.1.4.10 Transmission controls; A.3.7–3.9 Information transfer, identity, access; A.3.20–3.26 Security baseline	§6.4.6 Determine controls; §6.5.3 Implement privacy risk treatment plans
Do	Mitigation Strategies	Cybersecurity Integration	Applies APSIA methodology (Papamartzivanos et al. [35] integrating privacy and security. Aligned with ISO/IEC 27001:2022 ISMS baseline. Addresses C2, C7	§6.5.2 Treatment options including risk reduction through technical and organisational controls	Annex A Table A.3 (security controls from ISO/IEC 27001:2022 baseline); §0.2 Compatibility with ISO/IEC 27001 ISMS; A.3.11–3.12 Incident management	§4 Relationship with ISO/IEC 27001 and 27002 [69] (security controls drawn from these baselines)
DO—Documentation and Reporting (aligns with ISO 31000 §6.7 Recording and Reporting)						
Do	Documentation and Reporting	Comprehensive Documentation	Uses Data Privacy Vocabulary (Pandit [31]) for structured, reusable DPIA documentation. Addresses L2, C13, C15	§6.7 Recording and reporting (structured documentation of risk management process)	§7.5 Documented information; A.1.2.9 Records related to processing PII; A.3.14 Protection of records	§6.5.1 Prepare the report; §7 PIA report (full structure)
Do	Documentation and Reporting	Transparent Reporting	Establishes regular reporting protocols communicating DPIA findings to stakeholders and authorities. Addresses L2, C8, C15, S4	§6.7 Recording and reporting (communication with internal and external stakeholders)	A.1.3.4 Providing information to PII principals; §7.4 Communication	§6.5.2 Publication of the PIA; §7.6 PIA public summary
CHECK—Continuous Monitoring (aligns with ISO 31000 §6.6 Monitoring and Review)						
Check	Continuous Monitoring	Monitoring and Review	Implements automated monitoring and periodic audits, drawing on the continuous-assessment dimension of CLIFOD. Addresses C13	§6.6 Monitoring and review (effectiveness of risk management process and controls)	§9.1 Monitoring, measurement, analysis and evaluation; §9.2 Internal audit; §9.3 Management review; A.3.15 Independent review; A.3.25 Logging	§6.5.4 Review and/or audit of the PIA
CHECK—Compliance Verification (extends ISO 31000 §6.6 with privacy-specific compliance verification)						
Check	Compliance Verification	Legal Compliance Check	Verifies compliance with GDPR, EU AI Act, Data Act, local regulations (Article 29 Data Protection Working Party [12]; Richter [68]; (Moniz [37]). Addresses L1, L2, L3	Extends §6.6 Monitoring and review with privacy-specific legal/regulatory verification (not a discrete ISO 31000 step)	A.3.13 Legal, statutory, regulatory and contractual requirements; A.3.16 Compliance with policies, rules and standards	§7.4.6 Compliance analysis (dedicated section of PIA report)
Check	Compliance Verification	Fairness Validation	Applies fairness metrics (Calvi & Kotzinos [32]; Kasirzadeh & Clifford [52]) and proportionality (Moniz [37]), aligned with AI Act post-market monitoring. Addresses C6, C8, S1, S3	Extends §6.6 Monitoring and review with AI Act bias-monitoring verification (not a discrete ISO 31000 step)	Partial—A.3.16 validates adopted policies; A.1.3.11 addresses individual rights but not systemic fairness. Framework extends 27701	Not addressed—§7.4.6 is restricted to legal/regulatory compliance. Framework extends PIA toward fairness validation

Table A4. *Cont.*

Lifecycle Phase (PDCA)	Risk Management Domain	Control Objective	Operational Activity (Figure 4) and Addressed Challenges	ISO 31000:2018 Alignment (Process Backbone)	ISO/IEC 27701:2025 Mapping	ISO/IEC 29134:2023 Mapping
ACT—Review and Adaptation (aligns with ISO 31000 §6.6 Monitoring and Review—recurring/adaptive)						
Act	Review and Adaptation	Periodic Reviews	Regular review programmes incorporating regulatory and technological developments. Addresses L1, L2, C14	§6.6 Monitoring and review (periodic effectiveness review and process improvement)	§10 Improvement; §10.1 Continual improvement; §10.2 Nonconformity and corrective action; §9.3 Management review	§6.5.5 Reflect changes to the process; §6.2 Threshold analysis re-applied
Act	Review and Adaptation	Emerging Technologies	Adapts framework to AI, blockchain, IoT, big data developments. Addresses L2, L3, S3, S5, C14	§6.6 Monitoring and review (adaptive response to changes in external context, including emerging technology landscape)	§6.1.1 Actions to address risks (re-assessed when context changes); A.1.2.6 PIA triggered by new processing or changes	§6.5.5 Reflect changes (re-trigger PIA on significant technological change). Framework extends with dedicated emerging-tech treatment

The codes listed in Table A4 indicate the primary challenges addressed; the complete mapping is provided in Table A6 and Figure 4.

Table A5. Mapping of Phase 1 Challenge Taxonomy to Risk Management Domains of the proposed DPIA framework for AI-Driven Digitalisation.

Challenge Category	Specific Challenge Codes	Required DPIA Activity	Risk Management Domain
Legal and regulatory	L1, L2, L3	Compliance verification; legal scope definition	Compliance Verification; Pre-Assessment Phase
Risk assessment	R1, R2, R3, R4, R5, R6, R7	Risk identification, analysis and treatment	Risk Identification and Impact Evaluation; Mitigation Strategies
Complexity (risk-related)	C12, C13, C14	Risk treatment, monitoring and structured documentation	Risk Identification and Impact Evaluation; Mitigation Strategies; Documentation and Reporting (C13); Continuous Monitoring; Review and Adaptation (C14)
Complexity (collaboration)	C5, C9, C10	Continuous stakeholder engagement and interdisciplinary consultation	Pre-Assessment Phase (continuous Stakeholder Engagement, aligned with ISO 31000 §6.2 Communication and Consultation); Risk Identification and Impact Evaluation (Technical Feasibility, C5)
Complexity (implementation)	C1, C2, C3, C4, C6, C7, C8, C11, C15	Cross-cutting activities including risk analysis, fairness assessment, ethical analysis, cybersecurity integration, and structured documentation	Multiple domains (cross-cutting)
Scope (regulatory)	S3, S4	Compliance verification; regulatory adaptation	Compliance Verification; Review and Adaptation
Scope (stakeholder)	S1, S2	Contextual scoping; stakeholder consultation; ethical analysis	Pre-Assessment Phase; Risk Identification and Impact Evaluation
Scope (technological)	S5	Adaptation to emerging technologies and big data analytics environments	Review and Adaptation

Each Phase 1 challenge code is mapped to the specific Operational Activities that address it in the proposed framework (Figure 4), with the corresponding PDCA Phase and Risk Management Domain.

Table A6. Challenge-code-to-Operational-Activity traceability mapping.

Challenge Code	PDCA Phase	Risk Management Domain	Operational Activity (Figure 4)
L1	PLAN, CHECK, ACT	Pre-Assessment Phase; Risk Identification and Impact Evaluation; Compliance Verification; Review & Adaptation	Articulation of processing activities (Define Scope) [PLAN] Aligning processing with business goals (Define Objectives) [PLAN] Stakeholder Engagement [PLAN] Risk Policy [PLAN] Legal Compliance Check [CHECK] Periodic Reviews [ACT]
L2	PLAN, DO, CHECK, ACT	Pre-Assessment Phase; Risk Identification and Impact Evaluation; Documentation & Reporting; Compliance Verification; Review and Adaptation	Articulation of processing activities (Define Scope) [PLAN] Consideration of technological context (Define Scope) [PLAN] Aligning processing with business goals (Define Objectives) [PLAN] Addressing business needs (Define Objectives) [PLAN] Risk Policy [PLAN] Comprehensive Documentation [DO] Transparent Reporting [DO] Legal Compliance Check [CHECK] Periodic Reviews [ACT] Emerging Technologies [ACT]
L3	PLAN, CHECK, ACT	Pre-Assessment Phase; Risk Identification and Impact Evaluation; Review and Adaptation	Consideration of technological context (Define Scope) [PLAN] Ensuring data minimisation (Define Objectives) [PLAN] Technical Feasibility [PLAN] Legal Compliance Check [CHECK] Emerging Technologies [ACT]
R1	PLAN	Risk Identification and Impact Evaluation	Risk Policy [PLAN] Risk Analysis [PLAN]
R2	PLAN, DO	Pre-Assessment Phase; Mitigation Strategies	Data Flow Mapping [PLAN] Cybersecurity Integration [DO]
R3	PLAN, DO	Pre-Assessment Phase; Risk Identification and Impact Evaluation; Mitigation Strategies	Assessing data quality and sources (Define Objectives) [PLAN] Risk Analysis [PLAN] Cybersecurity Integration [DO]
R4	PLAN	Pre-Assessment Phase; Risk Identification and Impact Evaluation	Data Flow Mapping [PLAN] Risk Analysis [PLAN]
R5	PLAN	Risk Identification and Impact Evaluation	Risk Analysis [PLAN] User Rights Impact Analysis [PLAN]
R6	PLAN, CHECK	Risk Identification and Impact Evaluation; Continuous Monitoring	Risk Policy [PLAN] User Rights Impact Analysis [PLAN] Monitoring and Review [CHECK]
R7	PLAN	Risk Identification and Impact Evaluation	Risk Analysis [PLAN]
C1	PLAN, DO	Risk Identification and Impact Evaluation; Mitigation Strategies	Ethical Analysis [PLAN] Technical and Organisational Measures [DO]
C2	DO	Mitigation Strategies	Technical and Organisational Measures [DO] Cybersecurity Integration [DO]
C3	PLAN, DO	Pre-Assessment Phase; Risk Identification and Impact Evaluation; Mitigation Strategies	Data Flow Mapping [PLAN] Risk Analysis [PLAN] Technical and Organisational Measures [DO]
C4	PLAN	Pre-Assessment Phase; Risk Identification and Impact Evaluation	Addressing business needs (Define Objectives) [PLAN] Assessing data quality and sources (Define Objectives) [PLAN] Technical Feasibility [PLAN]
C5	PLAN	Risk Identification and Impact Evaluation	Technical Feasibility [PLAN]
C6	PLAN, CHECK	Risk Identification and Impact Evaluation; Compliance Verification	Fairness Assessment [PLAN] Ethical Analysis [PLAN] Fairness Validation [CHECK]
C7	PLAN, DO	Pre-Assessment Phase; Mitigation Strategies	Data Flow Mapping [PLAN] Cybersecurity Integration [DO]
C8	PLAN, DO, CHECK	Risk Identification & Impact Evaluation; Documentation & Reporting; Compliance Verification	Fairness Assessment [PLAN] User Rights Impact Analysis [PLAN] Transparent Reporting [DO] Fairness Validation [CHECK]
C9	PLAN	Pre-Assessment Phase	Stakeholder Engagement [PLAN]
C10	PLAN	Pre-Assessment Phase	Stakeholder Engagement [PLAN]
C11	DO *	Mitigation Strategies *	Not directly annotated in Figure 4; addressed implicitly through Technical Feasibility and Technical and Organisational Measures (see note).

Table A6. *Cont.*

Challenge Code	PDCA Phase	Risk Management Domain	Operational Activity (Figure 4)
C12	PLAN, DO, CHECK	Risk Identification and Impact Evaluation; Mitigation Strategies; Continuous Monitoring	Risk Policy [PLAN] Technical and Organisational Measures [DO] Monitoring and Review [CHECK]
C13	DO, CHECK	Mitigation Strategies; Documentation and Reporting; Continuous Monitoring	Technical and Organisational Measures [DO] Comprehensive Documentation [DO] Monitoring and Review [CHECK]
C14	ACT	Review and Adaptation	Periodic Reviews [ACT] Emerging Technologies [ACT]
C15	PLAN, DO	Risk Identification & Impact Evaluation; Documentation & Reporting	Risk Policy [PLAN] Comprehensive Documentation [DO] Transparent Reporting [DO]
S1	PLAN, CHECK	Pre-Assessment Phase; Risk Identification and Impact Evaluation; Compliance Verification	Stakeholder Engagement [PLAN] Fairness Assessment [PLAN] Ethical Analysis [PLAN] Fairness Validation [CHECK]
S2	PLAN	Risk Identification and Impact Evaluation	Ethical Analysis [PLAN]
S3	PLAN, CHECK, ACT	Pre-Assessment Phase; Risk Identification and Impact Evaluation; Compliance Verification; Review and Adaptation	Ensuring data minimisation (Define Objectives) [PLAN] Fairness Assessment [PLAN] Fairness Validation [CHECK] Emerging Technologies [ACT]
S4	PLAN, DO	Risk Identification & Impact Evaluation; Documentation & Reporting	Ethical Analysis [PLAN] Transparent Reporting [DO]
S5	ACT	Review and Adaptation	Emerging Technologies [ACT]

* C11 (lack of open-source DPIA tooling) is an environmental tooling challenge rather than a procedural one; it is therefore not annotated as a discrete code in Figure 4. It is supported implicitly through the Technical Feasibility activity (assessing the practicality of privacy-enhancing tooling) and the Technical and Organisational Measures activity (selecting and deploying available tooling).

Appendix C. Illustrative Application of the Proposed Framework: AI-Based Recruitment Screening and Ranking

In order to illustrate the operational logic of the suggested PDCA-based DPIA framework for AI-driven digitalisation, the following case study is provided. It builds upon previous work on privacy impact assessment as a tool for GDPR compliance preparation [70]. The sequence of events outlined has not been observed or verified in an organisational situation, therefore it does not represent empirical validation.

Context

A mid-sized professional services company with about 3500 workers made the decision to use a machine learning-based recruitment system to rank applicants for interviews and check resumes. The system was designed to improve uniformity in hiring decisions and shorten the time to shortlist. CV text, employment history, educational background, and, if freely provided, demographic information were to be processed. Early on, the organisation's legal and technology teams realised that the deployment presented serious regulatory issues under the EU AI Act, which categorises employment-related AI systems as high-risk, as well as the GDPR. The Data Protection Officer (DPO) formally suggested that a DPIA be carried out using the suggested methodology prior to go-live.

PLAN Phase

The decision to conduct a DPIA must be systematically documented before any substantive assessment is undertaken; Table A7 maps each WP248rev.01 triggering criterion against the system's specific characteristics in accordance with GDPR Article 35(1) (Article 29 Working Party [12]).

Table A7. DPIA Screening Checklist—AI-Based Recruitment Screening System (WP248rev.01 Criteria; Article 29 Working Party [12]).

No.	WP248rev.01 Criterion	Legal Reference	AI Recruitment System—Case-Specific Justification	DPIA Required?
1	Systematic and extensive profiling or automated decision-making with legal or similarly significant effects on individuals.	GDPR Art. 35(3)(a)	The ML system produces a ranked candidate shortlist that determines access to employment interviews. Shortlisting outcomes have direct and significant effects on individuals' access to employment.	YES—mandatory DPIA.
2	Large-scale processing of special categories of personal data (Art. 9) or criminal offence data (Art. 10).	GDPR Art. 35(3)(b)	Demographic data (ethnicity, disability status) is processed for fairness monitoring and held in a segregated data environment. Data covers all applicants across the organisation.	YES—mandatory DPIA.
3	Systematic monitoring of a publicly accessible area on a large scale.	GDPR Art. 35(3)(c)	Not applicable. The system processes CV data submitted by applicants; no public-area monitoring is involved.	NO.
4	Data concerning vulnerable data subjects who may be less able to freely consent or object.	WP248rev.01, Criterion 7	Candidates from non-traditional educational routes (apprenticeships, part-time degrees) were identified during stakeholder consultation as potentially vulnerable to algorithmic disadvantage.	YES—combined with No. 1, triggers DPIA.
5	Innovative or novel use of new technologies or organisational solutions.	GDPR Art. 35(1); WP248rev.01, Criterion 8	The ML-based CV ranking pipeline is a novel deployment with no prior use in the organisation's recruitment process.	YES—combined with No. 1, triggers DPIA.
6	Combining or matching data sets from two or more processing operations carried out for different purposes.	WP248rev.01, Criterion 6	Historical shortlisting records (ten years) are combined with current CV submissions and fairness-monitoring demographic data from a segregated store.	YES—combined with No. 1, triggers DPIA.
7	Processing that prevents data subjects from exercising a right or using a service or entering into a contract.	WP248rev.01 Criterion 9	A negative shortlisting outcome directly prevents candidates from accessing an employment opportunity, with potential financial and social consequences.	YES—mandatory DPIA.
DECISION	Two or more criteria satisfied. Criteria No. 1, 2, 4, 5, 6 and 7 are engaged.	GDPR [6] Art. 35(1); WP248rev.01, Section III.B.a	All applicable criteria confirm that a DPIA is mandatory prior to deployment of the AI recruitment screening system.	DPIA MANDATORY.

Pre-Assessment Phase

Define Scope | Define Objectives

The Head of HR Technology, legal counsel, and a representative from the Machine Learning (ML) provider attended the DPO's first scoping meeting. Within the first session, it became clear that the system triggered multiple Article 35 criteria requiring a DPIA. In particular, (i) it involved the large-scale processing of special category personal data, (ii) it deployed a new AI technology, and (iii) it produced decisions with significant effects on individuals' access to employment. The DPO formally documented the DPIA requirement and informed the relevant HR leadership.

The same meeting surfaced a tension that had not been anticipated. The provider had proposed using ten years of historical shortlisting data as the primary training corpus. However, legal counsel immediately pointed out that these historical records reflected a period during which the organisation's own shortlisting practices had systematically underrepresented candidates from certain universities and demographic backgrounds. The ML engineer confirmed that if the model were trained on that data without adjustment, it would learn to replicate those patterns. The organisation decided at this stage to commission a training data audit before any model training proceeded, a decision that directly delayed the project timeline by six weeks but which the DPO considered non-negotiable under the Fairness Principles Policy.

Simultaneously, the team decided to gather demographic information just for the purpose of evaluating fairness, including gender, ethnicity, and, if voluntary, disability status. They would not be involved in model scoring and would be kept in a segregated data environment with access restricted to the fairness monitoring function. This agreement was

formally documented as a commitment to GDPR [6] data protection principles, including purpose limitation.

Data Flow Mapping

The ML engineer and data architect were given a three-week deadline by the DPO to create a comprehensive data flow map. When the map was returned, it showed a problem that had not been apparent during the initial scoping: before being sent to the ranking model, candidate CV data was being routed through the cloud infrastructure of the third-party Applicant Tracking System (ATS) provider in a location outside the European Economic Area. No Article 28 GDPR [6] data processing agreement was in place, and no Chapter V GDPR [6] transfer safeguard (Articles 44–49) had been documented.

The DPO escalated this finding to the General Counsel. Consequently, the organisation paused the implementation timeline and required the provider to either (a) confirm that processing would remain within the European Economic Area (EEA), or (b) execute a Standard Contractual Clauses arrangement within thirty days. The provider agreed to restrict processing to European Economic Area (EEA) infrastructure. The Data Processing Agreement (DPA) was executed, and the data flow map was updated to reflect the revised architecture (see Table A8).

The legal team considered this one of the most operationally significant findings to emerge from the framework's pre-assessment activities, precisely because it would not have been surfaced by a conventional compliance review focused solely on internal data processing. The revised data flow map subsequently became a key governance artefact rather than merely a technical diagram. It provided visibility into the end-to-end processing chain, showing how candidate data moved from the ATS to the AI ranking engine and associated systems, and enabled the organisation to identify the involvement and geographical location of subprocessors. It also allowed the legal and privacy teams to anticipate the types of evidence that supervisory authorities could request regarding data flows, transfer mechanisms, access controls and retention responsibilities. As a result, the updated data flow map evolved into a governance instrument supporting traceability, accountability and regulatory preparedness throughout the lifecycle of the AI recruitment system. Table A8 maps each data asset against its governance parameters, including GDPR lawful basis and AI Act classification; transfer mechanism and processor records are documented in Tables A9 and A10 below (GDPR [6]; AI Act [7]).

Table A8. Comprehensive Data Inventory and Asset Register.

Business Process	Data Type	Data Owner	Shared Party (3rd Party)	Retention Period	Confidentiality (C)	Integrity (I)	Availability (A)	Risk Value	Lawful Basis (GDPR Art. 6)	AI Act Classification
CV Screening and Ranking	CV Text, Employment History	HR Technology	ATS Provider	During processing	High	High	Medium	High	Art. 6(1)(b)—Performance of contract (recruitment); Art. 6(1)(f)—Legitimate interest (fair hiring).	High-Risk AI System—Annex III, Point 4 (Employment and workers management).
Fairness Monitoring	Demographic Data (Gender, Ethnicity)	Monitoring Team	Not Shared	During monitoring	Very High	High	Low	Critical	Art. 5(1)(d) accuracy); Art. 6(1)(f)—Legitimate interest (fairness compliance), Art. 9(2) (where applicable for special category data).	Not an AI system—human-led monitoring process using demographic statistics only.

Stakeholder Engagement

The DPO recommended expanding the DPIA team to include functions other than legal and technical. Specifically, the DPO recommended including an external adviser specialising in algorithmic fairness and two representatives from employee resource groups that represent potentially affected communities. The Head of HR Technology initially resisted this, expressing concerns about the pace of the project and the risk of scope

creep. However, after the DPO led a discussion on the need to consider potential impacts on fundamental rights, including the potential implications of the EU AI Act's FRIA requirements, senior management endorsed the expanded team.

The representatives attended two structured consultation sessions. During the first session, they identified that the model's reliance on degree classification and university prestige as CV features would likely disadvantage candidates who had followed non-traditional educational routes, including apprenticeships and part-time degrees. In the second session, they raised concerns about the explainability of shortlisting decisions and noted that candidates who received no explanation for rejection might find it difficult to effectively exercise their rights under GDPR Articles 15 and 22 relating to automated decision-making. Both sets of findings were formally recorded and incorporated into the risk register and mitigation planning.

Although a Data Processing Agreement was executed with the ATS provider, no processor record existed at this stage for either the ATS provider or the ML vendor; Table A9 summarises the organisation's controller record of processing activities in accordance with GDPR [6], Article 30(1).

Table A9. Controller's Record of Processing Activities—GDPR [6] Article 30.

Service Code	Controller (Client) Details	DPO Contact (Processor)	Categories of Processing	Third-Country Transfers	Security Measures (TOMs)
SRV-ATS-01	Professional Services Organisation (3500 employees)—HR Technology Function. DPO: [Organisation DPO contact details].	dpo@ats-provider.eu	Applicant Tracking System: CV ingestion, storage, routing to ML ranking engine, delivery of ranked shortlists to HR managers. Access logging and retention scheduling.	Remediated: processing initially routed through non-EEA infrastructure. Following the pre-deployment audit, the provider agreed to restrict all processing to EEA infrastructure. No third-country transfers remained following remediation, eliminating the need for SCCs.	ISO/IEC 27001:2022 certified. AES-256 encryption at rest (remediated). Role-based access controls (RBACs). Access logs retained per ISMS requirements.
SRV-ML-01	Professional Services Organisation (3500 employees)—HR Technology Function. DPO: [Organisation DPO contact details].	dpo@ml-vendor.eu	ML model training on historical shortlisting data, fairness re-weighting, SHAP-based explainability layer generation, model inference for candidate scoring.	No third-country transfers. All processing within EEA.	Pseudonymisation of CV pipeline inputs. Demographic data technically isolated from inference pipeline. Automated deletion workflows for unsuccessful candidates.

The discovery of an undocumented cross-border data flow to third-country infrastructure was the most operationally significant pre-deployment finding; Table A10 provides the structured transfer tracker to document, where applicable, the transfer mechanism and TIA status for each processor.

Table A11 records each stakeholder concern against its framework challenge code and assigns monitoring ownership to a named function, providing the accountability traceability the PDCA governance model requires. Stakeholder participation supports multidisciplinary risk identification and impact assessment throughout the DPIA process (Mantelero [41]; Janssen et al. [36]).

Table A10. Cross-Border Transfer Tracker GDPR [6] Articles 28 and 46.

Processor/ Partner	GDPR Role	DPA (Art. 28) Status	Destination Country	Transfer Mechanism	TIA Status	Supplementary Safeguards
ATS Provider	Data Processor	DPA executed following pre-deployment audit finding; signed prior to go-live.	EEA (post-remediation). Original undisclosed destination: non-EEA third country.	Not applicable following remediation, as restricting processing to EEA infrastructure eliminated the need for a Chapter V transfer mechanism.	Not required following remediation, as no third-country transfers remained.	Contractual obligation on provider to notify any future infrastructure change outside EEA within 5 business days.
ML Vendor	Data Processor	DPA executed at contract signature.	EEA—no third-country transfer.	Not applicable.	Not required.	Model artefacts and training data held on EEA infrastructure under Role-Based Access Controls (RBACs).
Fairness Adviser	Independent Data Controller/Data Recipient	Data Sharing Agreement covering aggregate fairness statistics only. No individual-level data shared.	EEA.	Not applicable—aggregate statistics only; no personal data transferred.	Not required.	Adviser accesses aggregate outputs only; no access to candidate-level or demographic data.

Table A11. Stakeholder Engagement and Ethical Analysis Log.

Stakeholder Group	Identified Concern/Finding	Applied Mitigation/ Control Action	Challenge Code/Reference	Accountability/ Ownership
Employee Resource Groups	Educational route disadvantage due to reliance on degree classification and university prestige, including potential proxy discrimination arising from historical training data (Calvi & Kotzinos [32]).	Application of re-weighting techniques to reduce the influence of university prestige and degree classification in the training dataset.	C6—Algorithmic bias via feature weighting; S2—Structural disadvantage.	ML Engineer; DPO.

Table A11. *Cont.*

Stakeholder Group	Identified Concern/Finding	Applied Mitigation/ Control Action	Challenge Code/Reference	Accountability/ Ownership
Employee Resource Groups/External Ethics Adviser	Explainability of shortlisting decisions and risks of automation bias and candidates' ability to meaningfully contest AI-assisted decisions (Lazcoz et al. [51]; Janssen et al. [36]).	Deployment of SHAP value attribution; displaying candidates in alphabetical order; conducting HR manager training.	C9—Explainability; S1—Automation bias risk.	Head of HR Technology; ML Engineer.
External Ethics Adviser	Disadvantage for candidates with non-standard CV formats due to feature extraction pipeline calibration, potentially affecting data quality and representativeness (Calvi & Kotzinos [32]).	Interface redesign incorporated into the provider's scope of work.	C3—Data quality; S3—Input normalisation.	ATS Provider; HR Technology Lead.

Risk Identification and Impact Evaluation

Risk Policy | Risk Analysis

The full DPIA team convened to populate the risk register, with the ISO 31000-based Risk Management Policy serving as the governing standard. Four primary risks were identified and assessed in terms of their likelihood and potential impact on data subjects.

Table A12 documents both inherent and residual risk levels alongside treatment status, aligned with the ISO 31000:2018 risk management framework, enabling auditors to assess the effectiveness of applied controls.

Table A12. Risk Register and Assessment.

Risk ID	Identified Risk	Domain/ Regulatory Context	Likelihood	Impact	Overall Risk Level	Inherent Risk Level	Residual Risk Level	Treatment Status
R01	Proxy discrimination based on historical shortlisting data including risks arising from insufficiently representative training data (Calvi & Kotzinos [32])	Algorithmic Fairness, EU AI Act	High	High	Critical	Critical—no controls in place at assessment date.	Low—post fairness re-weighting and quarterly audit.	Treated. Re-weighting applied; quarterly fairness audit ongoing.
R02	Opacity of the scoring process making GDPR [6] compliance difficult, limiting meaningful explanation and contestability of AI-assisted decisions (Lazcoz et al. [51]; Calvi & Kotzinos [32]).	GDPR [6] Articles 13, 14, 15 and 22	High	Medium-High	High	High—no explainability mechanism at assessment date.	Low—post SHAP deployment and explainability portal.	Treated. SHAP deployed; candidate portal live.
R03	Data quality risk arising from structurally heterogeneous CV data.	GDPR [6] Article 5(1)(d)	Medium	Medium	Medium	Medium—heterogeneous CV formats degrading feature extraction.	Low—post interface redesign.	Treated. CV interface redesign completed pre-go-live.
R04	Re-identification risk associated with demographic attributes collected for monitoring.	GDPR [6] Articles 25 and 32	Low	High	Medium	Medium—demographic attributes accessible to monitoring environment prior to technical isolation.	Very Low—post technical isolation control and role-based access restrictions.	Treated. Demographic data technically isolated from inference pipeline; access restricted to authorised monitoring personnel.

The most significant finding concerned proxy discrimination. During this period, the training data audit commissioned at the scoping stage was completed and indicated that historical shortlisting rates were materially lower for candidates from less selective or

non-traditional higher education institutions than for candidates from more prestigious universities. The ML engineer assessed that, if the model were trained on this data without intervention, university type could emerge as a high-weight feature, effectively encoding institutional prestige as a proxy for candidate quality. This risk was categorised as having both a high likelihood and a high potential impact and was immediately reported to senior management and legal counsel.

A second risk concerned the opacity of the scoring process. The provider's original specification did not include any explainable output. Legal counsel noted that this would make compliance with GDPR [6] Articles 13–14 and Article 22 difficult to demonstrate, potentially leaving the organisation unable to respond meaningfully to requests for information about shortlisting decisions. The DPO rated this risk as having a high likelihood given the system's architecture and a medium-to-high impact given the expected annual volume of candidates to be processed.

Two further risks were identified as being of lower severity: a data quality risk arising from the self-reported and structurally heterogeneous nature of CV data; and a re-identification risk associated with the demographic attributes collected for fairness monitoring. These attributes could, if inadequately isolated, be inadvertently reintroduced into model training through indirect pathways.

Fairness Assessment

In order to address the risk of proxy discrimination in concrete terms, the fairness adviser and the ML engineer proposed a pre-deployment fairness testing protocol. Three metrics were selected. Demographic parity was chosen as a population-level check to detect gross disparity in shortlisting rates across groups. "Equal opportunity", which requires equal true positive rates across groups, was chosen as the primary metric because a violation of this metric would directly indicate that qualified candidates from protected groups were being advanced at lower rates than equally qualified candidates from the majority group, which was the main issue raised by the training data audit. Equalised odds was added to provide a fuller picture by also capturing disparities in false positive rates.

The team ran the model in a sandboxed environment against a test dataset consisting of historical applications for which actual hiring outcomes were available. The results indicated potential disparities. The demographic parity assessment suggested disparities in shortlisting outcomes for female candidates. Differences in equal opportunity were also observed between candidates from underrepresented groups and the majority group. The DPO presented these findings to the project steering committee and recommended that the model should not proceed to deployment in its current form.

Ethical Analysis

The external ethics adviser prepared a written analysis examining two risks that went beyond the quantitative fairness metrics. Firstly, she assessed the risk of automation bias. Even if the shortlist was formally subject to human review, HR managers presented with a ranked list under time pressure would be unlikely to routinely override the model's outputs. She recommended that candidates be presented in alphabetical order rather than ranked order in the interface design, to reduce anchoring effects, and that HR managers receive training on the limits of algorithmic outputs before the system goes live. Secondly, she found that candidates with non-standard CV formats, such as those structured around portfolio work rather than chronological employment, would be systematically disadvantaged by the model's feature extraction pipeline, which was calibrated to conventional CV structures.

Both findings were accepted by the steering committee. The interface redesign was incorporated into the provider's scope of work. A training programme for HR man-

agers was commissioned. The ethics adviser's written analysis was appended to the DPIA documentation.

User Rights Impact Analysis | Technical Feasibility

Legal counsel mapped the most operationally significant GDPR [6] rights under 15–22 against the system's operational design. The most significant gap identified was in respect of Article 22: the organisation needed to confirm that no shortlisting decision would be made solely by the automated system without human review. The provider's architecture was examined and it was confirmed that the system produced a ranked list, which a human recruiter was required to review and approve before any candidate was rejected. This was recorded in the DPIA as the primary safeguard for Article 22 compliance, subject to the condition that the interface redesign recommended by the ethics adviser was implemented before go-live.

The ML engineer and legal counsel assessed the technical feasibility of implementing an explainability layer. The engineer proposed using SHAP value attribution to generate candidate-level summaries of the features contributing to each score. A proof of concept confirmed that SHAP outputs could be generated within acceptable inference time limits and rendered in a format accessible to non-technical HR managers. The explainability layer was incorporated into the implementation scope.

Table A13 maps each legal requirement to its operational safeguard and records the evidence artefact and verification criteria required to demonstrate compliance; FRIA-specific elements under the AI Act [7] are documented in Table A14 below.

Table A13. Legal Compliance and Data Subject Rights Matrix.

Regulatory Framework	Specific Requirement/Right	System Feature/Operational Safeguard	Evidence Artefact	Verification Criterion
GDPR [6] Article 22	Protection against automated individual decision-making.	Ranked list requires human recruiter review and approval before any rejection (Human-in-the-loop).	HR manager shortlist approval log; system audit trail.	100% of shortlists reviewed by HR manager before any rejection; zero automated rejections without human sign-off.
EU AI Act [7]	Post-market monitoring requirements for high-risk AI systems.	Implementation of quarterly audits using live shortlisting data and an automated threshold-based alerting system.	Q1 and Q2 fairness audit reports; automated alerting system log.	Quarterly audit cycle completed on schedule; threshold alerts triggered within 24 h of breach.
GDPR [6] Articles 13-14	Right to be informed.	Publication of a public-facing summary on the careers portal and revision of candidate-facing language.	Careers portal privacy notice (revised); candidate-facing summary published.	Privacy notice reviewed annually; accessibility and accuracy verified by legal counsel (Janssen et al. [36]).

DO Phase

Mitigation Strategies

Table A13 addresses GDPR [6] and AI Act [7] compliance but does not incorporate the six FRIA elements specified under AI Act [7] Article 27(1) for applicable AI deployers; Table A14 provides this integrated assessment, drawing on the measures documented throughout the DO phase (AI Act [7]).

Table A14. Integrated AI DPIA and FRIA Evaluation—AI Act [7] Article 27(1) and GDPR [6] Article 35.

FRIA Element (Art. 27(1))	Legal Basis	Assessment Question	Implemented Measure	Review Frequency
Deployment process and intended purpose	AI Act [7] Art. 27(1)(a); Art. 13	How will the high-risk AI system be used, and does its use align with the provider's documented intended purpose?	System deployed as a candidate ranking tool for interview shortlisting, consistent with provider's Art. 13 instructions for use. HR manager review required before any rejection is applied (human-in-the-loop).	At each deployment scope change.
Period and frequency of use	AI Act [7] Art. 27(1)(b)	For how long and how frequently will the system operate, and are processing volumes proportionate to the stated purpose?	System operates continuously during active recruitment cycles. Volumes are proportionate to organisational hiring needs. Quarterly fairness audits are scheduled throughout the operational period.	Annually.
Categories of persons and groups likely to be affected	AI Act [7] Art. 27(1)(c)	Which individuals and groups are affected by the system, including those at particular risk of algorithmic disadvantage?	All external applicants. At-risk groups identified: candidates from non-traditional educational routes, female candidates (demographic parity monitoring), candidates from underrepresented ethnic backgrounds (equal opportunity monitoring). Intersectional analysis commissioned to identify potential compound disadvantage affecting individuals belonging to multiple protected groups (Calvi [53]; Janssen et al. [36]).	Following each quarterly audit.
Specific risks of harm to fundamental rights	AI Act [7] Art. 27(1)(d)	What are the specific risks of harm to non-discrimination, dignity, and access to legal remedy posed by the AI system?	R01: Proxy discrimination via institutional prestige weighting and insufficiently representative training data (Calvi & Kotzinos [32])—mitigated by fairness re-weighting (Tables A9, A12 and A15). Table A9 records re-weighting as a processing activity the vendor performs, whereas Table A15 frames it as an applied mitigation measure with an effectiveness KPI and residual-risk score, and A12 records the residual risk. R02: Opacity of scoring undermining Art. 22 rights—mitigated by SHAP explainability. R04: Re-identification of demographic attributes—mitigated by technical data isolation. Residual risk documented in Risk Register (Table A12).	Quarterly—aligned with fairness audit cycle.
Human oversight measures	AI Act [7] Art. 27(1)(e); Art. 26(2); GDPR [6] Art. 22	Who is responsible for oversight, do they have authority to override AI outputs, and have they received appropriate training?	Human recruiter reviews and approves ranked list before any rejection. Alphabetical candidate presentation reduces anchoring bias. HR manager training completed pre-go-live. DPO notified immediately on threshold breach; automated shortlisting suspended for affected role pending investigation (Table A12).	Pre-deployment + annually.

Table A14. *Cont.*

FRIA Element (Art. 27(1))	Legal Basis	Assessment Question	Implemented Measure	Review Frequency
Measures upon risk materialisation and complaint mechanism	AI Act [7] Art. 27(1)(f); Art. 86; GDPR [6] Art. 22(3)	What actions are taken if a risk materialises, and how can affected candidates seek remedy?	Escalation: automated threshold alert to DPO, Head of HR Technology, and ML Engineer simultaneously; automated processing suspension for affected role category. SHAP-based portal assists candidates to exercise their rights under GDPR [6] Art. 22(3) by providing meaningful information about the factors influencing the AI-assisted ranking. Complaint route published on careers portal. Governance log maintained (Table A13).	Annually + post-incident.

Technical and Organisational Measures

Following the PLAN-phase findings, the organisation implemented five measures before go-live. Table A15 documents each Technical and Organisational Measures (TOM) alongside its implementation date, effectiveness KPI and residual risk score, enabling auditors to assess both the completeness and the ongoing efficacy of the applied controls (ISO 31000:2018).

The training dataset was restructured. The ML engineer applied re-weighting techniques to reduce the influence of university prestige as a training signal and removed career gap duration as a standalone feature, replacing it with a composite employability indicator reviewed and approved by the fairness adviser. The model was retrained and the sandboxed fairness test was re-run. The results indicated improvements in fairness metrics and a reduction in disparities across groups, which the DPO and the steering committee considered acceptable subject to continued monitoring after deployment.

Table A15. Risk Treatment Plan and Applied Controls.

Targeted Risk	Applied Technical and Organisational Measure (TOM)	Responsible Function	Status	Implementation Timing	Effectiveness KPI	Residual Risk Score
R01	Application of re-weighting techniques to the training dataset to reduce the influence of university prestige.	ML Engineer	Completed	Pre-deployment—completed prior to go-live.	Demographic parity ratio ≥ 0.80 across all role categories; confirmed in Q1 fairness audit.	Low. Residual proxy discrimination risk managed through quarterly audit cycle.
R01, R04	Isolation of demographic attributes in a dedicated data store with role-based access control.	Data Architect/HR	Completed	Pre-deployment—completed prior to go-live.	Zero unauthorised access events; RBACs verified in Q1 security review.	Very Low. Re-identification risk effectively controlled by technical isolation.
R02	Deployment of a SHAP-based explainability layer connected to a candidate-facing portal.	ML Engineer/Legal Counsel	Completed	Pre-deployment—completed prior to go-live.	100% of shortlisting decisions accompanied by SHAP-based explanation accessible via candidate portal.	Low. Residual opacity risk for complex multi-feature interactions managed through DPO review.
Security	Remediation of outdated encryption at rest algorithms for CV data.	Information Security Team	Completed	Pre-deployment—remediated within 30-day window following pre-deployment audit finding.	AES-256 encryption verified by Information Security Team; confirmed in Q1 security audit.	Very Low. Encryption standard meets ISO/IEC 27001 requirements; no residual risk identified.
R03	Standardisation of CV submission format through structured application templates and interface redesign to improve feature extraction quality.	ATS Provider / HR Technology Lead	Completed	Pre-deployment—completed prior to go-live.	$\geq$95% successful feature extraction rate; no material parsing errors identified during Q1 validation.	Low. Residual data quality risk managed through periodic validation of CV parsing performance.

Demographic attributes were isolated in a dedicated data store with access restricted to the fairness monitoring team. An automated technical control was implemented to prevent any pathway by which demographic data could reach the scoring model's inference pipeline. The SHAP-based explainability layer was deployed and connected to a candidate-facing portal enabling shortlisted and rejected candidates to request a summary of the factors that had influenced their score. The CV processing pipeline was pseudonymised, with identifiable data held separately and accessible only to defined HR roles under role-based access control. Finally, automated deletion workflows were configured to remove unsuccessful candidate data in accordance with the retention schedule set out in the Privacy Policy.

Cybersecurity Integration

The organisation's information security team conducted an assessment of the ATS platform against the ISO/IEC 27001-based ISMS baseline. The assessment identified two gaps: the provider's logging configuration did not retain access logs in accordance with the organisation's ISMS requirements, and encryption at rest for CV data relied on an outdated algorithm. The provider was required to remediate both gaps before go-live. Remediation was confirmed in writing and recorded in the DPIA documentation.

Documentation and Reporting

Comprehensive Documentation | Transparent Reporting

The complete DPIA, including the risk register, fairness assessment findings, mitigation measures, stakeholder consultation records, and the ethics adviser's analysis, was finalised and signed off by the DPO and the General Counsel. A public-facing summary was published on the organisation's careers portal, informing candidates that an AI-assisted shortlisting process was in use, describing the safeguards in place, and providing a contact route for data subject rights requests. The DPIA documentation and related governance records were maintained in accordance with the organisation's internal governance procedures.

CHECK Phase

Continuous Monitoring

Monitoring and Review

The recruitment system went live and the fairness monitoring team conducted the first quarterly audit using live shortlisting data collected during the initial period of operation. The results were largely consistent with the pre-deployment assessment, with demographic parity and equal opportunity metrics remaining within the acceptable ranges established during the PLAN phase.

A subsequent quarterly audit produced a different picture. The demographic parity assessment indicated renewed disparities affecting candidates from underrepresented ethnic backgrounds for roles in the organisation's technology division. The automated alerting system flagged the issue and notified the DPO, the Head of HR Technology, and the ML engineer simultaneously. They promptly convened to review the underlying data. The ML engineer identified that the technology division had opened a large number of new roles requiring specific cloud computing certifications, a requirement that was not well represented in the historical training data. The model was effectively encountering a distribution shift for this role category, and its performance on underrepresented groups had degraded as a result.

The DPO suspended automated shortlisting for technology roles pending remediation. HR managers were instructed to conduct manual shortlisting for those roles during the interim period. The ML engineer developed a targeted recalibration of the model's feature weighting for technology roles, using a supplementary dataset sourced from the provider. Following recalibration and re-testing in the sandboxed environment, fairness metrics were

verified and shortlisting for technology roles resumed. The DPO recorded the incident in the governance log maintained under the DPIA framework.

Compliance Verification

Legal Compliance Check | Fairness Validation

Legal counsel conducted the first formal compliance review. The review confirmed continued alignment with the GDPR [6] obligations documented in the DPIA and with the EU AI Act's [7] post-market monitoring requirements for high-risk AI systems. One area requiring attention was identified: updated regulatory guidance on automated decision-making recommended that organisations provide candidates with a more specific explanation of their rights under Article 22 than the organisation's current careers portal text offered. Legal counsel drafted revised candidate-facing language, which was approved by the DPO and incorporated into the organisation's candidate-facing communications.

The fairness validation exercise aggregated the quarterly audit results and assessed them against the three selected metrics. Overall, the system demonstrated acceptable levels of demographic parity, with the exception of the previously identified technology role incident, which had been remediated. Differences in equal opportunity across the dataset remained within the range accepted during the PLAN phase. The DPO reported these findings to the steering committee and recommended continuation of the system subject to the annual DPIA review. The validation also demonstrated that fairness monitoring functioned as an iterative governance process rather than a one-off compliance exercise, with periodic reassessment supporting the continued effectiveness of deployed safeguards (Pandit [31]; Georgiadis & Poels [3]).

Table A16 documents fairness performance against defined quantitative thresholds and escalation trigger values for each metric, providing the continuous monitoring audit trail required under AI Act [7] Article 26(5) and 26(6) and GDPR [6] Article 35(11).

Table A16. Fairness Validation and Continuous Monitoring.

Evaluation Metric	Pre-Deployment (Sandbox)	Q1 Audit (Live)	Q2 Audit (Distribution Shift)	Remediation Action (ACT Phase)	Acceptable Threshold	Escalation Trigger
Demographic Parity	Potential disparities observed but addressed via re-weighting.	Within acceptable ranges.	Disparities affecting candidates from underrepresented ethnic backgrounds for technology roles.	Automated shortlisting suspended; manual shortlisting implemented temporarily.	Demographic parity ratio $\geq$ 0.80 (4/5ths rule; EEOC standard).	Ratio < 0.75 in any role category or across the overall shortlist.
Equal Opportunity	Differences initially observed, subsequently mitigated.	Within acceptable ranges.	Within acceptable ranges.	Model feature weighting recalibrated using a supplementary dataset. Model performance revalidated using updated fairness metrics before redeployment.	Equal opportunity difference $\leq$ 0.05 between protected and reference groups.	Difference > 0.08 sustained across two consecutive audit periods.
Equalised Odds	Maintained within acceptable ranges.	Consistent with pre-deployment.	Consistent with pre-deployment.	Continuous monitoring maintained.	Equalised odds difference $\leq$ 0.05 across protected and reference groups.	Difference > 0.10 in any single audit period.

ACT Phase

Review and Adaptation

Periodic Reviews | Emerging Technologies

The DPO convened the annual DPIA review. The review brought together the original DPIA team, including the external ethics adviser and the diversity network representatives, and examined the monitoring data collected during operation, the remediation incident affecting technology roles, updated guidance on automated decision-making, and a proposal from the HR technology team to enhance the system with a natural language processing module capable of analysing unstructured cover letter text.

The remediation incident was treated as the most significant governance finding of the review period. The steering committee concluded that the existing threshold-based alerting system had functioned as intended, but that the response protocol had been too slow for a system processing a substantial volume of candidates. A revised protocol was agreed, requiring immediate escalation to the DPO in the event of a threshold breach, with automated suspension of processing for the affected role category pending a decision. The Risk Management Policy was updated accordingly.

The proposed Natural Language Processing (NLP) module prompted a targeted reassessment of the Pre-Assessment Phase and Risk Identification domain of the framework. The DPO and the ML engineer identified that unstructured cover letter text introduced new risks not captured in the original risk register. In particular, there was a risk that the model might infer protected characteristics from language patterns, which the existing demographic feature isolation controls did not address. The steering committee decided not to approve the NLP module until a supplementary DPIA covering that specific enhancement had been completed. The DPO scheduled a supplementary assessment accordingly.

The annual review confirmed that the three selected fairness metrics were still appropriate for the system's current deployment context. However, diversity network representatives raised a new concern: the metrics currently used do not capture intersectional fairness. For example, they do not consider the experience of candidates who are both female and from an underrepresented ethnic background. A fairness adviser was commissioned to design an intersectional analysis to be incorporated into future audit protocols.

At the close of the review, the DPO formally documented the initiation of a new PDCA cycle. The results of the first cycle were used to inform the next cycle's PLAN phase. This included the remediation incident, updated regulatory guidance on automated decision-making, the deferred NLP module, and the intersectional fairness enhancement.

Table A17 records not only corrective actions but also the lessons learned, policy and control updates, and governance decisions that demonstrate the organisational learning the ACT phase is designed to produce.

Table A17. Incident Response and Continuous Improvement Log.

Phase/Date	Identified Incident/Finding	Corrective and Preventive Action (CAPA)	Lessons Learned	Policy/Control Update	Governance Decision
Q2 Audit (Live)	Distribution shift causing disparities for candidates from underrepresented ethnic backgrounds in technology roles.	Automated shortlisting suspended; manual shortlisting implemented; model recalibrated using a supplementary dataset.	Distribution shift in low-volume niche roles is not detected by existing demographic parity thresholds; role-category volume must be a separate monitoring dimension. Continuous monitoring should also account for changes in data distributions over time (Pandit [31]).	Monitoring protocol updated to include role-category volume thresholds; supplementary training dataset sourced for technology roles.	Steering committee approved temporary manual shortlisting for technology roles; model recalibration signed off by DPO before reinstatement.

Table A17. *Cont.*

Phase/Date	Identified Incident/Finding	Corrective and Preventive Action (CAPA)	Lessons Learned	Policy/Control Update	Governance Decision
Annual Review	Proposal for a Natural Language Processing (NLP) module to analyse unstructured cover letter text.	NLP module deferred pending a supplementary DPIA specifically covering inferential detection risks.	Novel inferential risks from unstructured text require a separate DPIA before any expansion of the feature set beyond structured CV data. Significant modifications to high-risk AI systems should prompt a renewed DPIA before deployment (Georgiadis & Poels [3]).	DPIA pre-approval policy formalised as a mandatory gate for all future feature additions to the ML pipeline.	Steering committee deferred NLP module pending supplementary DPIA; DPO scheduled assessment within 60 days.
Annual Review	Need for intersectional fairness metrics not captured by existing tools.	Fairness adviser commissioned to design an intersectional analysis for future audit protocols.	Single-axis fairness metrics are insufficient for detecting compound disadvantage; intersectional analysis must be built into the audit protocol from the outset. Intersectional discrimination may remain undetected where fairness monitoring relies solely on single-axis metrics (Calvi [53]).	Fairness audit protocol updated to include intersectional analysis from Q3 audit cycle onwards; fairness audit methodology updated to incorporate intersectional fairness assessment.	Steering committee approved commissioning of external fairness adviser to design the intersectional analysis methodology; approved implementation of the revised fairness monitoring methodology for future audit cycles.

Concluding Remarks

The organisation's first question when it set up its DPIA team to prepare for deployment was whether the AI system would generate accurate shortlists efficiently. With time however, it faced governance challenges that were quite different from those it had originally expected.

The audit of the training data exposed historical trends of underrepresentation correlated with institutional prestige, an issue not previously included on the original risk list. The data flow mapping exercise highlighted an un-noticed cross-border transfer issue, which necessitated changes to the provider's infrastructure before deployment could proceed. Diversity network representatives were consulted and raised concerns regarding automation bias and disadvantage by educational route that were not originally included in the risk register.

After deployment the organisation realised that fairness testing before deployment was not enough. Ongoing monitoring identified new disparities affecting tech roles, prompting a temporary pause in automated shortlisting, a model recalibration, and an update to escalation procedures. The incident highlighted how changes in distribution and recruitment could give rise to risks which could not have been foreseen at the time of the initial assessment.

Further complicating matters, an idea for a natural language processing module to analyse cover letters was suggested, which raised issues about inferential detection of protected characteristics. The enhancement was placed on hold pending a supplementary DPIA. At the same time, diversity network representatives noted that the current fairness metrics did not adequately capture intersectional disadvantage, which led to the development of an intersectional analysis approach.

References

1. Brunswicker, S.; Bertino, E.; Soein, M. Big Data for Open Digital Innovation—A Research Roadmap. *Big Data Res.* **2015**, *2*, 53–58. [CrossRef]
2. Hönigsberg, S.; Manhai Li, M.; Korneeva, E.; Wache, H.; Dinter, B. The impact of digital platform introduction on business models in SMEs—The interplay of efficiency and innovation orientation. *J. Strateg. Inf. Syst.* **2026**, *35*, 101967. [CrossRef]
3. Georgiadis, G.; Poels, G. Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Comput. Law Secur. Rev.* **2022**, *44*, 105640. [CrossRef]
4. Tikkinen-Piri, C.; Rohunen, A.; Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Comput. Law Secur. Rev.* **2018**, *34*, 134–153. [CrossRef]
5. Guillaume, O. Digitalisation, Safety and Privacy. In *Safety in the Digital Age*; Springer Briefs in Applied Sciences and Technology; Le Coze, J.C., Antonsen, S., Eds.; Springer: Cham, Switzerland, 2023. [CrossRef]
6. European Union. 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 (General Data Protection Regulation). Official Journal of the European Union. 2016. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679 (accessed on 15 April 2026).
7. European Union. Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. Available online: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed on 12 January 2026).
8. Neubauer, A.; Wynn, M.; Bown, R. AI, Authorship, Copyright, and Human Originality. *Encyclopedia* **2026**, *6*, 9. [CrossRef]
9. Rintamäki, T.; Golpayegani, D.; Lewis, D.; Celeste, E.; Pandit, H.J. Impact assessment requirements in the GDPR vs the AI Act: Overlaps, divergence, and implications. *Comput. Law Secur. Rev.* **2026**, *61*, 106317. [CrossRef]
10. Clarke, R. Privacy impact assessment: Its origins and development. *Comput. Law Secur. Rev.* **2009**, *25*, 123–135. [CrossRef]
11. Information Commissioner's Office. Conducting Privacy Impact Assessments Code of Practice. 2014. Available online: https://www.privacy-advocaat.nl/public/documents/184/ico-pia-code-of-practice.pdf (accessed on 16 March 2026).
12. Article 29 Data Protection Working Party. 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. Available online: https://ec.europa.eu/newsroom/article29/items/611236/en (accessed on 11 February 2026).
13. Hansen, M.; Runge, G.; Gruschka, N.; Jensen, M. Illuminating the DPIA Blackbox—A Survey of Data Protection Impact Assessment Practices in Organisations. In *Privacy Technologies and Policy. APF 2025. Lecture Notes in Computer Science*; Arastouei, N., Jensen, M., Rannenberg, K., Eds.; Springer: Cham, Switzerland, 2026; Volume 16183, p. 8. [CrossRef]
14. *ISO/IEC 27701:2025*; International Organization for Standardization, Information Security, Cybersecurity and Privacy Protection. Privacy Information Management Systems. Requirements and Guidance. International Organization for Standardization: Geneva, Switzerland, 2025. Available online: https://www.iso.org/standard/27701 (accessed on 12 January 2026).
15. Flick, U.; von Kardoff, E.; Steinke, I.; Jenner, B. *A Companion to Qualitative Research*; SAGE Publications: Thousand Oaks, CA, USA, 2004. Available online: https://books.google.com.tr/books?id=F6O-Ru4Ag1IC (accessed on 15 January 2026).
16. Thomas, D.R. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *Am. J. Eval.* **2006**, *27*, 237–246. [CrossRef]
17. Saunders, M.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*; Pearson: New York, NY, USA, 2019. Available online: https://www.scirp.org/reference/referencespapers?referenceid=2907709 (accessed on 24 December 2025).
18. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef] [PubMed]
19. Diepenbrock, S.S.A. Towards a Conceptual Framework for Data Protection Impact Assessments of Smart City Data Ecosystems. In Proceedings of the 2025 IEEE European Technology and Engineering Management Summit, Bruges, Belgium, 26–28 May 2025. Available online: https://www.researchgate.net/publication/392228520_Towards_a_Conceptual_Framework_for_Data_Protection_Impact_Assessments_of_Smart_City_Data_Ecosystems (accessed on 23 September 2025).
20. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering; Keele University, Keele, UK*; University of Durham: Durham, UK, 2007. Available online: https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering (accessed on 19 October 2025).
21. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. [CrossRef]
22. Mbozi, P.; Ratcliff, C.; Roberts, D. Critical Appraisal Skills Programme (CASP) Systematic Review Checklist. 2018. Available online: https://casp-uk.net/wp-content/uploads/2018/03/CASP-Systematic-Review-Checklist-2018_fillable-form.pdf (accessed on 13 March 2026).

23. *ISO/IEC 29134:2023*; Guidelines for Privacy Impact Assessment. International Organization for Standardization: Geneva, Switzerland, 2023. Available online: https://www.iso.org/standard/86012.html (accessed on 12 April 2026).
24. Huberman, A.; Miles, M.; Ritchie, J.; Spencer, L. *Qualitative Data Analysis for Applied Policy Research*; Sage: Thousand Oaks, CA, USA, 2022. [CrossRef]
25. Gale, N.K.; Heath, G.; Cameron, E.; Rashid, S.; Redwood, S. Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Med. Res. Methodol.* **2013**, *13*, 117. [CrossRef] [PubMed]
26. Goldsmith, L.J. Using Framework Analysis in Applied Qualitative Research. *Qual. Rep.* **2021**, *26*, 2061–2076. [CrossRef]
27. Jabareen, Y. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *Int. J. Qual. Methods* **2009**, *8*, 49–62. [CrossRef]
28. *ISO 31000:2018*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/65694.html (accessed on 15 March 2026).
29. Henriksen-Bulmer, J.; Faily, S.; Jeary, S. DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems. *Future Internet* **2020**, *12*, 93. [CrossRef]
30. Grammatopoulos, A.; Stylianou, I.; Barud, K.; Saillant, C.; Politis, I. TRUSTEE's Framework for DPIAs: Safeguarding personal information in the Digital Era. In Proceedings of the 2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, Edinburgh, UK, 6–8 November 2023. [CrossRef]
31. Pandit, H. A Semantic Specification for Data Protection Impact Assessments (DPIA). In *Towards a Knowledge-Aware AI. Studies on the Semantic Web*; Ebook; IOS Press: Amsterdam, The Netherlands, 2022; Volume 55, pp. 36–50. [CrossRef]
32. Calvi, A.; Kotzinos, D. Enhancing AI fairness through impact assessment in the European Union: A legal and computer science perspective. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, Chicago, IL, USA, 12–15 June 2023. [CrossRef]
33. Rehak, R.; Kuhne, C. The Processing goes far beyond "the app"—Privacy issues of decentralized Digital Contact Tracing using the example of the German Corona-Warn-App. In Proceedings of the 2022 6th International Conference on Cryptography, Security and Privacy, Tianjin, China, 14–16 January 2022. [CrossRef]
34. Leesakul, N.; Morisset, C. Position Paper: The role of law in achieving privacy and security measures in smart buildings from the GDPR context. In Proceedings of the 2023 IEEE European Symposium on Security and Privacy Workshops, Delft, The Netherlands, 3–7 July 2023. [CrossRef]
35. Papamartzivanos, D.; Menesidou, S.; Gouvas, P.; Giannetsos, T. A Perfect Match: Converging and Automating Privacy and Security Impact Assessment On-the-Fly. *Future Internet* **2021**, *13*, 30. [CrossRef]
36. Janssen, H.; Seng Ah Lee, M.; Singh, J. Practical fundamental rights impact assessments. *Int. J. Law Inf. Technol.* **2022**, *30*, 200–232. [CrossRef]
37. Moniz, G.C. DPIAs' role in fundamental rights governance. *Inf. Commun. Technol. Law* **2026**, *35*, 1–20. [CrossRef]
38. Campanile, L.; Iacono, M.; Marulli, F.; Mastroianni, M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Inf. Process. Manag.* **2021**, *58*, 102511. [CrossRef]
39. López, C.T.; Domingo, I.A.; Torrijos, J.V. 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, 17–20 August 2021. [CrossRef]
40. Georgiadis, G.; Poels, G. Establishing a Comprehensive Data Protection Impact Assessment Methodology for Big Data Analytics in Compliance with the General Data Protection Regulation. *Inf. Syst. E-Bus. Manag.* **2025**, *24*, 87–132. [CrossRef] [PubMed]
41. Mantelero, A. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Comput. Law Secur. Rev.* **2018**, *34*, 754–772. [CrossRef]
42. Bisztray, T.; Gruschka, N.; Mavroeidis, V.; Fritsch, L. *Data Protection Impact Assessment in Identity Control Management with a Focus on Biometrics*; Gesellschaft für Informatik e.V.: Bonn, Germany, 2020. Available online: https://www.researchgate.net/publication/342304096_Data_Protection_Impact_Assessment_in_Identity_Control_Management_with_a_Focus_on_Biometrics (accessed on 12 February 2026).
43. Gültekin-Várkonyi, G. Navigating data governance risks: Facial recognition in law enforcement under EU legislation. *Internet Policy Rev.* **2024**, *13*, 1–36. [CrossRef]
44. Riemann, L.T.; Hähner, F.P.S.; Schmitz, A.-K.; Ataian, M.; Jaster, M.; Ückert, F. An Open-Source Software Tool to Facilitate Data Protection Impact Assessments. *Appl. Sci.* **2023**, *13*, 11230. [CrossRef]
45. Wright, D.; Hert, P. *Privacy Impact Assessment*; Springer: Berlin/Heidelberg, Germany, 2012. [CrossRef]
46. Johnson, R.; Onwuegbuzie, A. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educ. Res.* **2004**, *33*, 14. [CrossRef]
47. Vemou, K.; Karyda, M. Evaluating privacy impact assessment methods: Guidelines and best practice. *Inf. Comput. Secur.* **2019**, *28*, 35–53. [CrossRef]

48. Bryman, A. Integrating Quantitative and Qualitative Research: How Is It Done? *Qual. Res.* **2006**, *6*, 97–113. [CrossRef]
49. 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 *Annual Privacy Forum*; Springer: Cham, Switzerland, 2016. Available online: https://www.researchgate.net/publication/319276698_A_Process_for_Data_Protection_Impact_Assessment_under_the_European_General_Data_Protection_Regulation (accessed on 23 April 2026).
50. Campanile, L.; Iacono, M.; Marulli, F.; Mastroianni, M. Privacy Regulations Challenges on Data-centric and IoT Systems: A Case Study for Smart Vehicles. In *IoTBDS*; SciTePress: Setúbal, Portugal, 2020. [CrossRef]
51. Lazcoz, G.; Maiora, J.; de Miguel, Í.; Sanz, B. Regulating AI-Driven Triage: Fundamental Rights and Compliance Challenges in the European Union. *AI* **2026**, *7*, 86. [CrossRef]
52. Kasirzadeh, A.; Clifford, D. Fairness and Data Protection Impact Assessments. In Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society, Virtual Event, 19–21 May 2021. [CrossRef]
53. Calvi, A. Gender, data protection & the smart city: Exploring the role of DPIA in achieving equality goals. *Eur. J. Spat. Dev.* **2022**, *19*, 24–47. [CrossRef]
54. Jong, B.; Gaye, B.; Luyten, J.; Buitenen, B.; André, E.; Meehan, C.; O'Siochain, C.; Tomsu, K.; Urbain, J.; Peeters Grietens, K.; et al. Ethical Considerations for Movement Mapping to Identify Disease Transmission Hotspots. *Emerg. Infect. Dis.* **2019**, *25*, e181421. [CrossRef] [PubMed]
55. Mittelstadt, B.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L. The Ethics of Algorithms: Mapping the Debate. *Big Data Soc.* **2016**, *3*, 2053951716679679. [CrossRef]
56. Binns, R. Fairness in Machine Learning: Lessons from Political Philosophy. In Proceedings of the Conference on Fairness, Accountability and Transparency, New York, NY, USA, 23–24 February 2018. Available online: https://proceedings.mlr.press/v81/binns18a.html (accessed on 29 January 2026).
57. Custers, B.; Dechesne, F.; Sears, A.M.; Tani, T.; van der Hof, S. A comparison of data protection legislation and policies across the EU. *Comput. Law Secur. Rev.* **2018**, *34*, 234–243. [CrossRef]
58. *ISO/IEC 27001:2022*; International Organization for Standardization, Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/27001 (accessed on 12 May 2026).
59. Irish Data Protection Commission. Data Protection Impact Assessments. Available online: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments (accessed on 11 May 2026).
60. Information Commissioner's Office. What is a DPIA? 2022. Available online: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/ (accessed on 10 May 2026).
61. National Commission on Informatics and Liberty. Carrying Out a Data Protection Impact Assessment when Necessary. 2023. Available online: https://www.cnil.fr/en/carrying-out-protection-impact-assessment-if-necessary (accessed on 12 May 2026).
62. Personal Data Protection Commission Singapore. Guide to Data Protection Impact Assessments. 2021. Available online: https://www.pdpc.gov.sg/organisations/resources/guidance-by-topic/guide-to-data-protection-impact-assessments (accessed on 15 May 2026).
63. Office of the Privacy Commissioner of Canada. Expectations: OPC's Guide to the Privacy Impact Assessment Process. Available online: https://www.priv.gc.ca/en/privacy-topics/federal-government-privacy/privacy-impact-assessments/gd_exp_202003/ (accessed on 15 May 2026).
64. Information Commissioner's Office. Sample DPIA Template. 2018. Available online: https://ico.org.uk/media2/migrated/2553993/dpia-template.docx (accessed on 15 May 2026).
65. Nissenbaum, H. Privacy as Contextual Integrity. *Wash. Law Rev.* **2004**, *79*, 119. Available online: https://nissenbaum.tech.cornell.edu/papers/H.%20Nissenbaum,%20_Privacy%20as%20Contextual%20Integrity.pdf (accessed on 12 January 2026).
66. UK-Government. Research and Analysis Cyber Security Risks to Artificial Intelligence. 2024. Available online: https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/cyber-security-risks-to-artificial-intelligence (accessed on 17 February 2026).
67. European Union Agency for Network and Information Security. Guideline on Security Measures Under the EECC. 2021. Available online: https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc (accessed on 27 May 2026).
68. Richter, H. Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing. *GRUR Int.* **2023**, *72*, 458–470. [CrossRef]

69. *ISO/IEC 27002*; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/75652.html (accessed on 24 June 2026).
70. Metin, B.; Erkan, S.; Atasu, İ.; Yılmaz, E. Privacy Impact Assessment as a Tool for GDPR Compliance Preparation. *Kişisel Verileri Koruma Derg.* **2019**, *1*, 75–86. Available online: https://dergipark.org.tr/en/download/article-file/904860 (accessed on 13 April 2026).