This is a submitted manuscript of the following conference paper:
Hills, A, Da Veiga, A, Loock, M & Renaud, K 2024, A holistic list of privacy-preserving measures for system development life cycles.
in *Advanced Research in Technologies, Information, Innovation and Sustainability: Fourth International Conference, ARTIIS 2024, Santiago de Chile, Chile, October 21-23, 2023, Proceedings.* Communications in Computer and Information Science, Springer, Cham.

A Holistic List of Privacy-Preserving Measures for System Development Life Cycles

Alida Hills, Adele Da Veiga, Marianne Loock and Karen Renaud

Abstract. Personal information, as a key resource for companies, must be kept confidential as per the relevant data protection regulations. The same data protection regulations provide employees and customers the right to control their personal information. IT software is used to create, edit, store, and delete this personal information. However, cyber-attacks, security concerns, and data breaches relating to the personal information of customers and employees occur at an alarming rate, violating the confidentiality and privacy of said customers and employees. Privacy by Design (PbD) should be embedded into traditional Information Technology (IT) software development life cycles (SDLCs) to minimise data loss or breaches of personal information to aid in ensuring end-to-end privacy and confidentiality of personal data. Moreover, IT software must comply with data protection regulations to minimise data loss or breaches of personal information. A scoping literature review was conducted to gain insight into PbD and data protection regulations principles that are embedded into IT SDLC phases. Relevant articles were analysed using a qualitative approach. Privacy-preserving measures are identified that can be used to meet the PbD and data protection regulations requirements. The contribution of this paper is a holistic list of privacy-preserving measures that can be utilised to embed privacy considerations data protection regulations into the IT SDLC phases.

Keywords: Software development life cycle (SDLC), Privacy, Privacy by design (PbD), Data protection regulations

1 Introduction

The worldwide increase in theft and misuse of personal information, often facilitated by security and privacy flaws in IT software, is lamentable. Data breaches have a negative impact on organisations, as privacy concerns can result in stock price reduction, the loss of customers, fines, additional costs to address the consequences, and the loss of trust by customers, who might abandon the company [24]. Data protection legislation has been enacted world-wide to aid in addressing the right to privacy and to protect personal information. In 2019, this legislation increased from 120 to 139 laws worldwide. In 2021, 132 of 194 countries had put legislation in place to secure the protection of data and privacy [14]. To keep up with the pace at which IT technology and systems develop and change, current legislation must evolve. This results in an ongoing strengthening of legislation to confirm that software developers take care when developing IT software to ensure that it is privacy-aware [28].

Personal information is processed by technology (it is created and stored by utilising IT software) on behalf of those with legitimate access (with authentication mechanisms ensuring legitimate access). Data protection regulations, such as the General Data Protection Regulation (GDPR), require that the personal information of customers and employees is used properly and fairly and make privacy a legal

requirement for the processing of such personal information. Embedding privacy and data protection regulations into the SDLC used for IT software development can assist with the protection of personal information in IT software. Although privacy protection should be woven into the software throughout the SDLC, it is difficult to determine how this ought to be achieved, in other words, the operationalisation of a PbD approach is not yet standard practice. The objective of this research is to propose a holistic list of privacy-preserving measures across SDLC phases. Privacy-preserving measures are defined as controls that can be implemented across the SDLC phases to assist development teams in ensuring privacy (aligned with PbD and data protection regulations) when developing IT software.

This paper is structured as follows: Section 2 states the research problem and derives the research question, Section 3 provides background information for PbD, the SDLC, and data protection legislation. Section 4 outlines the scoping literature review and Section 5 presents the research findings. Section 6 acknowledges limitations and suggests future work. Section 7 concludes.

2 Research Problem and Research Question

Data protection regulations adopted by various countries make data privacy a legal requirement for the processing of personal information. IT software uses SDLCs to enable the processing of personal information, and privacy should be embedded into SDLCs to assist in the development of privacy-aware software. Data protection regulations are applicable to the development of IT software that processes personal information. Article 25 of the GDPR embeds personal information security and PbD into the complete life cycle of an organization's systems (interpreted as the SDLC), products, and services [13, 16]. Even though research exists that identifies privacy-preserving measures to embed privacy and data protection regulations into the SDLC phases, there is still a general lack of methodological support, tools, and processes to embed privacy [20]. To operationalise PbD, it must be translated into feasible tools and processes (e.g., the SDLC) and applied to existing controls, guidelines, and standards [10]. When analysed, the existing research does not present a single or standardised holistic list of privacy-preserving measures to embed privacy and data protection regulations into the SDLC phases. The holistic list of privacy-preserving measures proposed in this study can guide IT software developers to assist in developing privacy-aware IT systems as it will provide the focus and understanding required by the development team to operationalise PbD across the SDLC phases (Requirements, Analysis and Design, Code/Develop (Implementation), Testing/Verification, Deployment, and Maintenance). The following research question was formulated to support the contribution of the paper: *What would a holistic list of privacy-preserving measures comprise that should be considered to embed privacy and data protection regulations into IT SDLC phases?*

3 Background Information

The IT software industry is growing and changing rapidly, as is the number of cyber-attacks and data breaches globally. IT software processes huge volumes of personal data, resulting in significant benefits, but at the risk of the individual's privacy. This

makes privacy a critical attribute and requirement to consider in the context of data privacy and security. Privacy in IT software development is criticised, as it is still in development and not operationalised yet. There is no standard way proposed to implement privacy in IT software development, many developers lack skills and training, and there is a general lack of methodological support and tools for dealing with privacy across all phases of the SDLC [12], [20], [23].

Another way to assist in operationalising privacy and security in IT system development is to create a privacy and security mindset. The IT system development team must be educated in privacy and security, and a mindset must be created to support the development of privacy-aware IT software. Four viewpoints are suggested to be applied to the standard Waterfall SDLC phases to evaluate, through a self-assessment method, if and how an organisation adopts a privacy mindset in IT software development. The result of the self-assessment is a list of checkpoints for PbD, namely, acknowledging privacy across the organisation (across all the SDLC phases); transparency about the appropriate privacy policies (actively enforced across all the SDLC phases); privacy built in through the Analysis & Design and Code/Develop (Implementation) phases of the SDLC; and enabling end-user control over their personal data collected by the IT system across the Analysis & Design and Code/Develop (Implementation) phases of the SDLC [6]. A tool was built with privacy, assurance, and accountability principles that can be used to educate development teams on good privacy practices using technology, policies, and regulations. This tool assists in identifying the privacy considerations that should be designed in the software [11]. Training was added as an additional phase to emphasise that the development team must understand security and regulations, as it will empower them to develop secure software [17]. The need for a privacy or security mindset in IT software development can be satisfied by adding these privacy-preserving measures into the various SDLC phases. IT software must protect personal data and privacy, and one way to accomplish this is to apply the PbD approach to embed privacy into the SDLC from the start. Another approach is to apply data protection legislation principles that provide individuals with rights regarding the privacy of their personal information and obligations, that entities must adhere to when processing personal data of individuals into the SDLC.

3.1 Privacy by Design (PbD) Approach

Ann Cavoukian, the then Ontario information and privacy commissioner, created the PbD approach in the mid-1990s [10]. It is viewed as the international privacy standard, to be added to data protection regulations to ensure data privacy [10]. The approach aims to prevent privacy infringements, such as unauthorised storage, disclosure, and usage of the data in IT software development before it happens. The SDLC is one of the processes used to develop IT software. The PbD principles that relate to the SDLC are that privacy should be included during IT software development by default and pro-actively, and that it is to remain intact through the SDLC to ensure protection of personal information by the final software product. Privacy should not be added as an afterthought, but be embedded into the software throughout the SDLC, when the architecture and design of IT software is achieved [11].

3.2 System Development Life Cycle (SDLC)

The SDLC is a process used when IT software is developed. Examples of SDLC models include the V-model, Agile, Waterfall, Spiral, Iterative, Incremental, Prototyping, Rapid Application development (RAD), and Scrum. The typical SDLC phases are Requirements, Analysis and Design, Code/Develop (Implementation), Testing/Verification, Deployment, and Maintenance [19].

3.3 Data Protection Legislation

The GDPR (Article 25) was selected as the data protection legislation to be used in this study, as it is one of the most well-known data protection laws [12]. It came into force in May 2018, is regarded as a data law milestone [30] and is widely regarded as a privacy law for the world, playing an increasingly prominent role across the globe. The GDPR replaced the 1995 EU Data Protection Directive, which was the former worldwide data protection benchmark. The directive prohibited the transfer of personal information to non-EU countries (international data transfers) that did not have adequate protection measures for the processing of personal information [27]. The GDPR requires all countries that handle European citizens' personal information to ensure the protection thereof when such data is collected, stored, and processed [16]. The rights of the data owners, as stipulated by the GDPR, must be respected, and organisations that collect and manage the personal information must keep it confidential [23].

4 Scoping Literature Review

A scoping literature review was conducted to enable the identification and understanding of the extensiveness of the existing literature and to assist in identifying gaps in extant research [21, 31]. The scoping literature review incorporated the PRISMA-ScR. As per this reporting protocol, the information sources are described (e.g., the databases used with dates or period of access); the potentially relevant articles are identified and extracted; the articles and documents are screened and assessed for eligibility, are either included in the review or excluded, with reasons; and the process is presented by a flow diagram [25]. In this research, articles for PbD and GDPR principles embedded into SDLCs, as privacy-preserving measures, were reviewed. The keywords are presented in table 1.

Table 1. Keywords used in searches

Keywords		Combinations (keywords AND this column)
Privacy OR Privacy by Design	AND	Software development life cycle (SDLC) OR Software development OR System development
GDPR	AND	IT software development OR IT system development OR Software development life cycle (SDLC) OR Software engineering
Data protection OR Data privacy OR Data security OR Software security	AND	Software development life cycle (SDLC)

The literature search across the identified sources includes results of peer-reviewed papers for the past twelve years (since 2011/2012 to 2023), written in English. Results prior to 2011/2012, especially for PbD and SDLCs, were included as exceptions when

they were deemed to add value to the research. Reverse referencing was used when a relevant reference was found in an article or articles. Exclusions were done based on relevance of the topic, the abstract, the introduction, and the conclusion. Studies were excluded if it did not address the GDPR in the context of IT software development. Similarly, studies were excluded if they did not address PbD in the context of IT software development. One hundred and thirty-six records were identified through database searching. These included journal articles, conference papers, and theses. Alternative words were used to increase the results. Ninety-eight remained for screening after 38 duplicates were removed. Fifty-four records were excluded as they did not address the GDPR or PbD in the context of SDLCs, or were written before 2011; however, they were included when deemed to add value to the research. This left 44 full-text articles to be assessed for eligibility, of which 22 were excluded with reasons based on the quality of the study and the fact that no privacy-preserving measures across the SDLC phases were identified in the articles. The articles included in the qualitative analysis, where privacy-preserving measures were identified across the SDLC phases, were 22 [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23, 26, 29].

5 Research Findings

A proposed holistic list of privacy-preserving measures was identified from the consolidated literature review. The types of privacy-preserving measures that were discussed in the various articles are depicted in Figure 1. Each one of these types provided privacy-preserving measures that are, or can be, added to the SDLC phases.

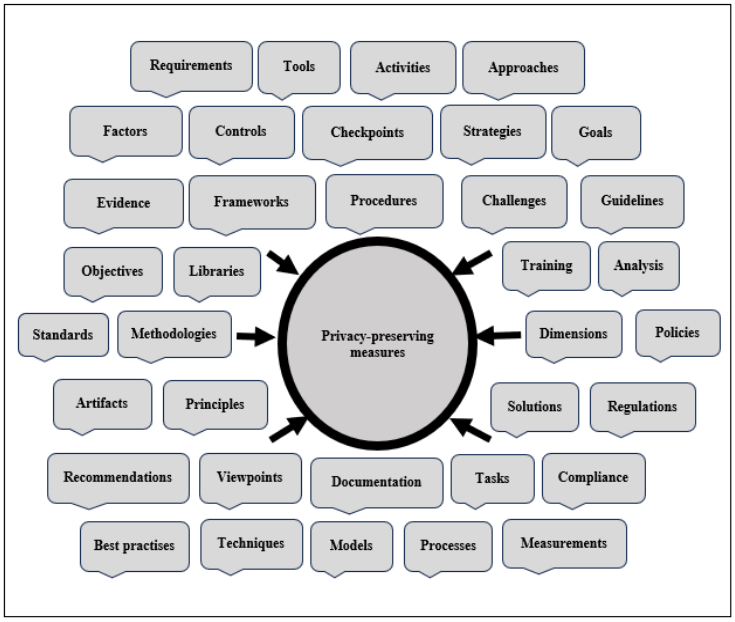

Fig. 1. Types of privacy-preserving measures

The sections that follow present an overview of the research findings of existing work in which privacy-preserving measures were identified, to answer RQ1. The privacy-preserving measures include PbD principles and data protection regulations that have been added, or are proposed to be added, into the SDLC phases.

5.1 What would a holistic list of privacy-preserving measures comprise that should be considered to embed privacy and data protection regulations into IT SDLC phases??

Business processes are designed in the Requirements phase of the SDLC and updated in the Maintenance phase (after deployment of the IT software). Surveys reported in the literature focused on the design of business activities, specifically, business process management in the Requirements and Maintenance phases [26]. Four strategies that can be used by companies to implement PbD or develop a framework for PbD, were identified. The strategies are based on the SWOT (strengths, weaknesses, opportunities, and threats) analysis and include offensive (strengths and opportunities), defensive (strengths and threats), re-orientation (weaknesses and opportunities), and survival (weaknesses and threats) strategies to be used to implement PbD. These privacy-preserving measures can be added to the two identified SDLC phases. Privacy requirements gathering during the Requirements phase, and updating thereof throughout the SDLC, were identified through 78 studies that used various methodologies and tools to support this action. This is required for IT software to comply with data protection regulations and to provide the required privacy to the individuals involved [8]. These privacy-preserving measures were added to the Requirements phase in the proposed holistic list.

Risk management activities were incorporated into various SDLCs approaches, such as Waterfall, the V-model, prototypes, and RAD, to ensure a robust and secure SDLC. Examples of the risks that were considered are improper design, poor user interface, and an unqualified testing team [1]. Effective risk management for security threats is ensured by introducing known security controls into the development process [15]. Risk management is one of the privacy-preserving measures identified that was added to the various SDLC phases.

Various privacy-preserving measures were embedded into various SDLC phases. Twenty-one security rules were identified, from as early as 2009, that were implemented in software to assist in eliminating vulnerabilities and ensure more secure software; one of these rules was privacy. Rules include Awareness, Accountability, Integrity, Non-repudiation, Accuracy, Authorisation, Assessment/evaluation, Flexibility, Unambiguity, Auditability, Prevention, Confidentiality, Availability, Access control, Identification & authentication, Consistency, Privacy, Excellence, Fortification, Error classification, and Interoperability [5]. Although privacy was integrated into the Agile and Waterfall SDLCs, a privacy-aware/privacy-enhanced W-model that integrates PbD into the SDLC phases, was proposed [3]. This is done through PRIPARE (Preparing Industry to Privacy by Design by supporting its Application in Research) as a PbD methodology with eight phases: Analysis, Design, Implementation, Verification, Release, Maintenance, Decommissioning, and Environment/ Infrastructure [3]. New

stages were added as a critical part of this model: the privacy analysis where a Privacy Impact Assessment (PIA) is done in the PRIPARE Analysis phase, the Privacy-enhancing architectures (PEAR) in the PRIPARE Design phase, which was then implemented and verified in the PRIPARE Implementation and Verification phases [3]. Artifacts that can be used as privacy-preserving measures for PbD and GDPR principles were introduced in a working draft document, compiled for software engineers, to provide guidance in documenting functional and non-functional privacy objectives and controls throughout the SDLC phases [9]. All the above privacy-preserving measures were added to the proposed holistic list.

The SSDLC (Secure Software Development Life Cycle) adds the security dimension as another layer to the normal SDLC [15] and improves the security quality of the software. Two approaches are proposed, namely, Pro-active to prevent breaches at the start of the SDLC, and Re-active to maintain security throughout the SDLC. These privacy-preserving measures were added to ensure that security is included by the time the software is implemented [15]. The MS-SDL (Microsoft Security Development Life Cycle) is a best practise model that can be used for secure development through the Waterfall SDLC, as security is included in each phase [17].

A framework that specifies the level of the SSDLC required, through the CIA (functional Correctness, safety Integrity and security Assurance) level, based on the Security-by-Design framework, combines the SSDLC with an evidence-based security approach (where evidence includes documentation such as security training plans, design specifications, unit test results, user guides, and vulnerability response plans) [18]. Detailed security activities (e.g., tools and techniques, policy approval, system protection, encryption key management, access control) and evidence are used to determine the required level of the SSDLC. Ten phases and 66 security activities and evidence (from standards, laws, rules, target market and regulations) were derived across the SDLC phases and added to the activity-evidence mapper. The database is the repository for the mapping results. The CIA level (one to seven) is determined by the CIA-level extractor, which uses the database to construct a customised SSDLC [18]. The documentation (evidence) and activities were added to the proposed holistic list as privacy-preserving measures.

The SSD (Software Security Development) approaches identified security concerns across the SDLC phases. Secure development recommendations were added to resolve the concerns and embed security principles into the complete SDLC, resulting in Security Requirements, Security Design, Security Development, Security Testing, Security Deployment, and Security Maintenance phases by adding activities, issues and challenges, security tasks, and solutions per phase [2]. As per the above, privacy-preserving measures such as PRIPARE, PIAs, PEAR, artifacts, privacy objectives and controls, and secure software development are embedded in the SDLC phases. All the above privacy-preserving measures were added to the proposed holistic list.

Various approaches and frameworks were identified to be used in implementing PbD across SDLC phases. Best practices, in the Analysis and Design phase of the SDLC, were reviewed and some of the PRIPARE project results were discussed, with

a specific focus on this phase. Guidelines direct the elicitation of the privacy requirements that assist in achieving the privacy targets. These requirements result in the design of measures or privacy controls [22]. The aim of PRIPARE is to provide a framework for the development of privacy-friendly and user-centric IT software. It merged existing best practices for PbD into a single framework with two dimensions: the first is the SDLC phases (Requirements, Analysis and Design, and Testing/verification) as a goal-based approach, and the second is the activities. The PEAR process is used to enhance the privacy architecture to achieve the business objectives and privacy goals, ensure security, and avoid privacy risks. A PIA and a risk-based approach are used to elicit privacy requirements [22]. Techniques were identified to assist in ensuring privacy in IT software, including Privacy Enhancement Techniques (PETs), privacy policies, design patterns, strategies, and PIAs [23]. The PRIPARE privacy methodology was also discussed in this context. The methodology covers the following phases of the SDLC: Analysis and Design, Code/develop (Implementation), Testing/verification, Deploy, Maintenance, and Decommission, along with two additional phases that cover the Environment/Infrastructure. The PIA is integrated through the SDLC from the Analysis and Design phase and includes risk management. PETs relate to technical measures that should be implemented to secure data, such as encryption and pseudonymisation [23]. The proposed holistic list of privacy-preserving measures provides a good indication of where these measures were added into the SDLC phases.

An integrated framework, to introduce privacy management in IT software development, was based on people-process-technology and integrates into the SDLC, using the SDLC as a guideline [29]. Areas that impact privacy in IT software development projects include the three Privacy management frameworks (PMFs) for PbD as a goal-based, risk-based, and policy-based approach, Privacy technical frameworks (PTFs), Privacy tools and libraries (PTLs), Privacy awareness (PA), and Privacy measurement (PM). The proposed integrated framework consists of seven consecutive phases and three supportive processes. The seven consecutive phases include Project planning, Requirement specification, Analysis, Design, Coding, Testing, and Deployment. Supportive processes include project monitoring and control that will provide ongoing tracking of the privacy status, project risk management that will assess the risk factors for breaches, and privacy requirement management [29]. The security level of the developed system will significantly increase when security is added to each phase of the SDLC through Privacy Oriented Software Development (POSD), by using the Privacy Knowledge Base (PKB) [4]. The PKB privacy-preserving measures include PbD principles, design strategies, patterns, vulnerabilities, and context. Privacy-preserving measures for the phases include a PIA, security software architecture, privacy design strategies, patterns, and architectural requirements. It also includes PETs, static code analysis (SCA) to identify any vulnerabilities produced during coding, and penetration testing (PENTEST) to verify the security level of the overall system. Platform hardening was added as building blocks to the later SDLC phases [4]. The proposed holistic list of privacy-preserving measures provides a good indication of where these were added to the SDLC phases.

Privacy-preserving measures were identified to embed GDPR principles in IT SDLCs, where the legal requirements of PbD principles in the GDPR (Article 25) are translated into technical solutions by the APSIDAL framework [7] (**A**ccountability, **P**urpose Limitation, **S**torage Limitation, **I**ntegrity and Confidentiality, **D**ata Minimization, **A**ccuracy, **L**awfulness, Fairness and Transparent). The three phases of the framework are Preparation, Assessment, and Implementation [7]. In the Preparation phase, the DPIA (data protection impact assessment) is done to identify the impact of processing on an individual's personal information. In the Assessment phase, legal compliance with the GDPR is assessed using the seven GDPR principles (lawfulness, purpose limitation, data minimisation, storage limitation, integrity and confidentiality, accuracy, and accountability). In the Implementation phase, the final privacy requirements are implemented into IT software development and the required environments [7]. Article 25 of the GDPR lists seven factors to be considered when the legal compliance with the GDPR is checked. The factors include state of the art technology, nature, cost, context, scope, risks, and purpose [13]. The improved APSIDAL framework balances its focus towards the data life cycle. The following three factors were added to be considered when the legal compliance with the GDPR is checked: complexity, usability, efficiency, and effectiveness, bringing the total to 11 factors [7]. The framework factors and phases were added to the proposed holistic list of privacy-preserving measures.

Privacy-preserving measures identified in the updated APSIDAL framework, to elicit data protection and privacy requirements, include threat modelling during the Analysis and Design phase of the SDLC, and vulnerability assessment, PENTEST, and static and dynamic code reviews in the Maintenance phase [7]. The output from the Assessment phase (the privacy requirements for the IT software development and required environments) can be used as input into, or privacy-preserving measures for, the SDLC to develop and implement the software [7]. The identified privacy-preserving measures were added to the two identified SDLC phases in the proposed holistic list.

To align the SDLC with the data protection regulations (GDPR principles), a process consisting of six procedures/documents that provides the mandatory requirements to embed privacy of personal information in IT software, is proposed where these are added to the six SDLC phases (Requirements, Design and Analysis, Development, Testing, Deployment, and Maintenance), providing the controls to embed PbD [14]. These privacy-preserving measures were added to the SDLC phases in the proposed holistic list.

5.2 Embedding Privacy-preserving Measures and Data Protection Regulations into IT SDLC Phases

Table 2 presents a view of the types of privacy-preserving measures (activities, tasks, solutions, frameworks, etc), linked to the SDLC phases. The SDLC phases, as listed in the tables below, include the standard phases of Requirements, Analysis and Design, Code/develop (Implementation), Testing/verification, Deployment, Maintenance, and Decommissioning. New phases proposed in the literature review were added (Training, and Environment/Infrastructure phases).

A holistic list of privacy-preserving measures for system development life cycles

Table 2. The types of privacy-preserving measures linked to the SDLC phases

Training -New	**Requirements**		**Analysis and Design**	**Code/Develop (Implementation)**
Activities	Activities Analysis Approaches Artifacts Best practises Challenges Checkpoints Compliance Controls Dimensions Documentation Frameworks Goals Guidelines Libraries	Measurements Methodologies Models Objectives Policies Principles Procedures Processes Regulations Requirements Solutions Standards Strategies Tasks Tools Viewpoints	Activities Analysis Approaches Artifacts Challenges Compliance Controls Documentation Evidence Goals Methodologies Models Policies Principles Procedures Requirements Solutions Strategies Tasks Viewpoints Feed from APSIDAL framework	Activities Artifacts Challenges Controls Documentation Procedures Processes Solutions Tasks Viewpoints
Testing/ Verification	**Deployment**	**Maintenance**	**Decommissioning**	**Environment/ Infrastructure - New**
Activities Analysis Artifacts Challenges Compliance Controls Documentation Evidence Goals Procedures Recommendations Solutions Tasks Techniques Viewpoints	Activities Artifacts Challenges Controls Documentation Evidence Policies Procedures Solutions Tasks Viewpoints	Activities Artifacts Documentation Evidence	Activities Artifacts Documentation Evidence	Activities

Table 3 presents a proposed holistic list of privacy-preserving measures to embed privacy and data protection regulations into the SDLC phases, as extracted from the articles in the literature review. The types of privacy-preserving measures are indicated in the SDLC phases (as per Table 3), along with the measures associated in the articles (quality gates, data classification, implement the PEAR, etc). The existing privacy-preserving measures, identified from the literature review, were added as bullets to the relevant phases to propose a holistic list across the SDLC phases. The list can be used to guide IT software developers in understanding when and how privacy should be embedded into the different SDLC phases when developing privacy-aware software. This can assist in creating the privacy awareness required to provide a basic understanding and knowledge of privacy principles and data protection regulations, to empower the team to include it in the development. The proposed holistic list can also be used to guide the IT software development team to operationalise privacy when developing IT software.

A holistic list of privacy-preserving measures for system development life cycles

Table 3. A proposed holistic list of privacy-preservative measures that should be considered to embed privacy and data protection regulations into IT SDLC phases

Training phase (new phase) • Add privacy training as an additional phase at the start of the SDLC [17].
Requirements phase • Risk management activities [1], e.g., analyse security and privacy risk and define quality gates [17]. • Security challenges, solutions, and tasks (sources of security requirements, data classification, use and misuse case modelling, risk management) [2]. • Privacy enhanced activities [3], privacy requirements [8], [20]. • Privacy Knowledge Base (PKB): PbD principles, strategies, vulnerabilities checkpoints, context analysis [4]. • Documentation/artifacts - PIA [4]; stakeholder list, privacy requirements, privacy RACI, purposes for collection and processing, including retention of personal information, use cases/user stories, models of data flows, procedures, processes, and behaviours internal and external to the software for platforms interaction, APIs, imported code, description of contextual visibility and transparency at the point of interaction with the user/data for data collection, use, and disclosure [9]; and DPIA, standards, guidelines, frameworks, methodologies, compliance with legal framework, measurements of impact and risk, activities to address privacy issues, threats, and privacy patterns [22]. • 21 Security rules [5]. • Four viewpoints: acknowledge privacy in the organisation, appropriate privacy policies, build privacy in, enable end-user control [6]. • Accountability-based privacy governance and controls, assurance and external reviews controls, technology objectives, policies, best practises, laws and compliance, regulations, training, tools, guidelines, fair information principles (FIPs) artifacts [11]. • Documentation/Artifacts • Procedure for Requirements Analysis: SDLC and GDPR [14]. • Tracking activities [15]. • CIA security activities and evidence (documentation) [18]. • Activities: functional description and high-level privacy analysis, promote privacy awareness activities, PRIPARE methodology [23]. • Four strategies: SWOT, offensive, defensive, re-orientation, survival [26]. • People-technology-process approach triad: privacy tools and libraries (PTLs), privacy awareness (PA) activities, process privacy management frameworks (PMFs), goal-based approach, risk-based approach, policy-based approach, privacy measurement (PM) [29].
Analysis and Design phase • Risk management activities [1]. • Security challenges, solutions, and tasks (core security design considerations, additional design considerations, threat modelling) [2]. • PIA, PEAR design documentation [3]. • 21 Security rules [5]. • Four viewpoints: acknowledge privacy in the organisation, appropriate privacy policies, build privacy in, enable end-user control [6]. • Secure software activities, PbD strategies, privacy patterns activities, architectural requirements [4], privacy requirements [20]. • Threat modelling [7], [13], [17], attack surface analysis [17]. • Documentation/artifacts: privacy design principles, architecture, user interface (UI) design, traceability of personal information collected, state-of-the-art privacy properties included in designs, describe user/data subject privacy options including (access) controls, preferences/settings, UI support, and user/data subject-centric privacy model, describe notice, consent, and other privacy interactions at the EARLIEST possible point in a data transaction exchange with a user/data subject or the automated agent or device [9]. • Procedure for Design Phase: SDLC and GDPR [14]. • Pro-Active: risk assessment activities [15]. • CIA security activities and evidence (documentation) [18].

- Top-down approach, bottom-up approach, horizontal approach, PEAR design documentation, privacy principles, level of compliance, applicability of privacy requirements, goal-based approach, risk-based approach, legal compliance [22].
- Privacy architecture documentation, policies, design patterns activities and strategies, legal assessment/compliance, privacy and security plan preparation, detailed privacy analysis, activities to operationalise privacy principles, risk management activities, PEAR design and PIA documentation, privacy enhancing detail design documentation, promote privacy awareness activities, PRIPARE methodology [23].
- PbD approach [29].

APSIDAL framework: DPIA documentation, legal compliance with GDPR (lawfulness, purpose limitation, data minimisation, storage limitation, integrity and confidentiality, accuracy, accountability), policies, procedures, processes, legal measures, access limitations, data completeness awareness, data normalisation policy, data management, training and awareness, data life span, identity and access management, encryption, physical security, strategy, standards and best practises, awareness and education, certification in IT products and services, embedded transparency, legal measures, non-repudiation services, data inventory measures, centralised storage, data pseudonymisation, stripping of unused metadata, intermediary proxies, data dispute handling and cleansing, traceability, end-to-end encryption, data validation, authentication, authorisation, tamper proof audit trails, monitoring, data loss prevention. Factors: state of the art technology, nature, cost, context, scope, risks, purpose, complexity, usability, efficiency, effectiveness, (Output of Assessment phase feeds to SDLC), compliance with GDPR Article 25 [7], [13].

Code/Develop (Implementation) phase

- Risk management activities [1], e.g., analyse security and privacy risk, define quality gates [17].
- Security challenges, solutions, and tasks (common software vulnerabilities and controls, secure software processes, secure build environments) [2].
- Privacy enhanced activities, implement the PEAR [3].
- PETs, processes [4].
- 21 Security rules [5].
- Four viewpoints: acknowledge privacy in the organisation, appropriate privacy policies, build privacy in, enable end-user control [6].
- Documentation/artifacts: security and privacy in the developed software, organization and partnering organizations, measurements for usage and effectiveness of privacy controls to ensure continuous improvement [9].
- Procedure for Development Phase: SDLC and GDPR [14].
- Pro-Active: threat modelling and design review tasks [15].
- CIA security activities and evidence (documentation) [18].
- Privacy implementation tasks, PETs processes (technical measures, e.g., encryption), promote privacy awareness activities, PRIPARE methodology [23].
- PTLs, PTFs artifacts [29].

Testing/Verification phase

- Risk management activities [1].
- Security challenges, solutions, and tasks (attack surface validation, test data management) [2].
- Privacy enhanced activities, verify system against the requirements [3].
- 21 Security rules [5].
- Two of the four viewpoints: acknowledge privacy in the organisation, appropriate privacy policies [6].
- Static code analysis (SCA) and penetration testing (PENTEST) techniques [4], Pro-active: static analysis recommendations [15].
- Documentation/artifacts: tests for meeting privacy objectives when implementing privacy controls [9].
- Procedure for Testing Phase: SDLC and GDPR [14].
- Dynamic/fuzz testing controls, verify attack model/threat surface [17].
- CIA security activities and evidence (documentation) [18].
- Validation and verification of adherence to conformance/compliance with the requirements, goal-based approach, risk-based approach, legal compliance [22].

• Accountability, security and privacy dynamic, and static analysis dimensions, promote privacy awareness activities, PRIPARE methodology [23].
Deployment phase • Risk management activities [1]. • Security challenges, solutions, and tasks (software acceptance considerations, validation and verification, certification, and accreditation (C&A), installation) [2]. • Privacy enhanced activities [3]. • 21 Security rules: [5]. • Two of the four viewpoints: acknowledge privacy in the organisation, appropriate privacy policies [6]. • Documentation/artifacts: deployment environment, state-of-the-art privacy properties included in implementations [9], create incident response plan, system decommissioning plan, final security, and privacy review, publish PIA report [23]. • Procedure for Deployment Phase: SDLC and GDPR [14]. • Reactive: security testing and code review tasks [15]. • Response plan, final security review, release archive evidence (documentation) [17]. • CIA security activities and evidence (documentation) [18]. • Encryption and security controls addressed in last phases [20]. • System hardening control [4], vulnerability scan and system hardening tasks, privacy deployment process and procedure, privacy continuity plan (artifact) [29].
Maintenance phase • Security challenges, solutions, and tasks (operation, monitor and measure, incident, problem, change management, disposal) [2]. • Privacy enhanced activities, response plans [3]. • Two of the four viewpoints: acknowledge privacy in the organisation, appropriate privacy policies [6]. • Vulnerability assessment, PENTEST, static and dynamic code reviews [7], [13]. • Documentation/artifacts: security and privacy in the monitoring software, organization, and partnering organizations, measurements for software monitoring: usage and effectiveness of privacy controls to ensure continuous improvement [9]. • Procedure for Maintenance Phase: SDLC and GDPR [14]. • Reactive: security assessment and secure configuration activities [15]. • Response execution activities [17]. • CIA security activities and evidence (documentation) [18]. • Evidence of executing incident response plan, security, and privacy verifications [23]. • Four strategies: SWOT, offensive, defensive, re-orientation, survival [26].
Decommissioning phase • Documentation/artifacts: response plans [3], software retirement plan [9]. • Reactive: response plan 15]. • CIA security activities and evidence (documentation) [18]. • Execute decommissioning plan [23].
Environment/Infrastructure phase (new phase) Advocate and enhance privacy-awareness in the organisation units (activities) [3].

6 Limitations and Future Work

The information presented in the proposed holistic list is based on the results of the scoping literature review. As it is still conceptual, an expert review must be conducted to validate the proposed holistic list. A conceptual framework should be developed and validated to provide support to developers and to address privacy concerns when privacy-aware software is developed [20]. A framework that will provide a guide that can be used by IT software developers to implement PbD can be developed [23] (in the context of mobile health applications). The application of the proposed APSIDAL framework in different environments and IT software development to evaluate, expand, and improve the framework is suggested [13]. This can include the integration

of the framework into existing practices and management systems within the organisation; the framework can be expanded to include PbD across multiple jurisdictions and regulations and not only the GDPR and EU, and how to embed privacy in legacy IT systems. Future studies can be done to compile a best-practices document that includes tools and mechanisms, based on the list of checkpoints, to map PbD to the checklists and identify any gaps [6].

7 Conclusion

This research presented a proposed holistic list of privacy-preserving measures that can be used to guide how to embed privacy and data protection regulations in IT software development. Future work can focus on the development of a framework, which will be further validated with an expert panel. The list of the proposed privacy-preserving measures that were identified can operationally support the development team as a guide when privacy-friendly IT software is developed, as it can make them aware of how privacy and related data protection regulations can or should be embedded into the SDLC phases.

References

1. Agarwal, P., Singhal, A., Garg, A.: SDLC Model Selection Tool and Risk Incorporation. Int J Comp Appl 172(10), 6–10 (2017).
2. Alhuqail, S.K., Jamail, N.S.M.: Implementation of an Effective Framework in Merging Cybersecurity and Software Engineering. Sixth International Conference of Women in Data Science 2023, pp. 31–36. IEEE, Prince Sultan University (WIDS PSU) (2023).
3. Al-Momani, A., Kargl, F., Schmidt, R., Kung, A., Bösch, C.: A privacy-aware V-model for software development. Security and 2019, pp. 100–104. IEEE (2019).
4. Baldassarre, M.T., Barlette, V.S., Caivano, D., Piccinno, A.: Integrating Security and Privacy in HCD-Scrum. CHItaly: 14TH Biannual Conference of The Italian Sigchi Chapter 2021, pp. 11–13. ACM, New York (2021).
5. Banerjee, C. Pandey, S.K.: Software Security Rules, SDLC Perspective. IJCSIS 6(1), 123–128 (2009).
6. Bernsmed, K.: Applying Privacy by Design in Software Engineering – A European Perspective. The Second International Conference on Advances and Trends in Software Engineering (SOFTENG) 2016, pp. 69–76. IARIA (2016).
7. Blix, F., Elshekeil, S.A., Laoyookhong, S.: Designing GDPR Data Protection Principles in Systems Development. J Int Tech and Sec Trans 6(1), 548–555 (2018).
8. Canedo, E.D., Bandeira, I.N., Calazans, A.T.S., Costa, P.H.T., Cançado, E.C.R., Bonifácio, R.: Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. Req Eng 28(2), 177–194 (2023).
9. Cavoukian, A., Carter, F., Jutla, D., Sabo, J., Dawson, F., Fieten, S., Fox, J., Finneran, T.: Annex Guide to Privacy by Design Documentation for Software Engineers Version 1.0, http://docs.oasis-open.org/pbd-se/pbd-se-annex/v1.0/, last accessed 2023/10/01.
10. Cavoukian, A.: Privacy by Design. Leading edge 31(4), 18–19 (2012).
11. Cavoukian, A., Taylor, S., Abrams, M.E.: Privacy by Design: essential for organizational accountability and strong business practices. IDIS 3, 405–413 (2010).
12. De Chaves, S.A., Benitti, F.B.V.: Privacy by Design in Software Engineering: An update of a Systematic Mapping Study. Symposium on Applied Computing. Association For Computing Machinery 2023, pp. 1362–1369. ACM/SIGAPP, Tallinn, Estonia (2023).
13. ElShekeil, S.A., Laoyookhong, S.: GDPR Privacy by Design - From Legal Requirements to Technical Solutions, https://dsv.su.se/en/about/news/dsv-students-rewarded-for-master-thesis-in-the-field-of-it-security-1.351719, last accessed 2023/08/14.

14. Freitas, M.B., Araújo, V.M., and Magalhães, J.P.: Process SDLC-GDPR: Towards the Development of Secure and Compliant Applications 1ST International Conference on Advanced Innovations in Smart Cities (ICAISC) 2023, pp. 1–6. IEEE (2023).
15. Fujdiak, R., Mlynek, P., Mrnustik, P., Barabas, M., Blazek, P., Borcik, F., Misurec, J.: Managing the Secure Software Development. IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2019, pp. 1–4. IEEE (2019).
16. General Data Protection Regulation 2016/679, https://eur-lex.europa.eu/homepage.html, last accessed 2023/07/06.
17. Jøsang, A., Ødegaard, M., Oftedal, E.: Cybersecurity through secure software development. Ifip World Conference on Information Security Education, Advances in Information and Communication Technology, WISE 2015, vol 453, pp. 53–63. Springer, Cham (2015).
18. Kang, S., Kim, S.: CIA-level driven secure SDLC framework for integrating security into SDLC process. J Ambient Intell Human Comput, 13(10), 4601–4624 (2022).
19. Khan, P.M., Beg, M.M.S.S.: Extended Decision Support Matrix for Selection of SDLC-models on Traditional and Agile Software Development Projects. International Conference On Advanced Computing And Communication Technologies (ACCT) 2013, pp. 8–15. IEEE (2013).
20. Morales-Trujillo, M.E., Matla-Cruz, E.O., García-Mireles, G.A., Piattini, M.: Privacy by Design in software engineering: A systematic mapping study. CiBSE, 107–120 (2018).
21. Munn, Z., Peters, M.D.J., Stern, C., Tufanara, C., McArthur, A., Aromataris, E.: Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Meth 18, 1–7 (2018).
22. Notario, N., Crespo, A., Martín, Y., Del Alamo, J.M., Le Métayer, D., Antignac, T., Kung, A., Kroener, I., Wright, D.: PRIPARE: Integrating privacy best practices into a privacy engineering methodology. IEEE Security and Privacy Workshops 2015, pp. 151–158. IEEE (2015).
23. Okoye, J.N.: Privacy by design, https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2457831, last accessed 2023/09/20.
24. Pelteret, M., Ophoff, J.: Organizational information privacy strategy and the impact of the POPI act. Information Security for South Africa (ISSA), 56–65 (2017).
25. Rethlefsen, M.L., Kirtley, S., Waffenschmidt, S., Ayala, A.P., Moher, D., Page, M.J., Koffel, J.B.: PRISMA-S: an extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews. Systematic reviews: 10(1), 1–19 (2021).
26. Romero, S., De-Pablos-Heredero, C.: Contribution of Privacy by Design (of the processes). Harv Deusto Bus Res 6(3), 176–191 (2017).
27. Roos, A.: The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected "Content Principles". Comp Int Law J South Afr 53(3), 1-37 (2020).
28. Rustad, M.L., Koenig, T.H.: Towards a global data privacy standard. Fla L Rev 71(2), 365–454 (2019).
29. Sakul-Ung, P., Smanchat, S.: Towards Privacy Framework in Software Development Projects and Applications: An Integrated Framework. Research, Invention, And Innovation Congress (RI2C) 2019, IEEE (2019).
30. Schwartz, P.M.: Global Data Privacy: The EU way. N Y Univ Law Rev 94, 771-818 (2019).
31. Xiao, Y., Watson, M.: Guidance on Conducting a Systematic Literature Review. J Plan Educ Res 39(1), 93–112 (2019).