National College of Ireland

Data Privacy in Buy Now Pay Later (BNPL) - A Comprehensive PIA Framework

MSc Research Project
MSc in Cyber Security

Meril Antony
x23103418

School of Computing
National College of Ireland

Supervisor: Kamil Mahajan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Meril Antony
Student ID:	X23103418
Programme:	MSc in Cyber Security **Year:** 2024
Module:	MSc Research Project
Supervisor:	Kamil Mahajan
Submission Due Date:	29/01/2025
Project Title:	Data Privacy in Buy Now Pay Later (BNPL) - A Comprehensive PIA Framework
Word Count:	6524 **Page Count** 21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Meril Antony
Date:	29/01/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Assessing Data Privacy in Buy Now Pay Later (BNPL) - A Comprehensive PIA Framework

Meril Antony
x23103418

Abstract

The rapid expansion of the BNPL sector has introduced unique set of privacy challenges, concerning the usage, processing, and sharing of user data. This study develops a tailored Privacy Impact Assessment (PIA) framework specific to the BNPL sector, integrating privacy-by-design principles and ISO/IEC 27701 standards. The research employs systematic layers that includes a custom data mining tool, risk assessment matrix and a qualitative evaluation using the PEGS methodology. These tools identify key risks that arises from extensive data collection, third-party sharing, cross-border transfers, and automated decision-making practices. The tailored framework ensures compliance with GDPR and international standards while focusing on transparency, accountability, and privacy solutions. Evaluation of the framework by PEGS method demonstrated high efficiency. Future research aims to include stakeholder engagement to refine the privacy practices. This research largely contributes to advancing privacy frameworks for Fintech ecosystem, safeguarding user data in a digital era.

1. Introduction

The rising popularity of Fintech have seen a massive impact on the financial market and consumer behaviour. During the covid-era, when digital markets reached its peak, there was an increased focus on a particular Fintech that integrates financial platforms with non-financial platforms, Buy Now, Pay Later (BNPL) Services. Young crowds were particularly attracted to this service due to its user-friendly credit experience as observed by (Tan, 2022), providing them the opportunity of enhanced consumer payment options. BNPL services are now integrated with almost all the retail platforms from goods to services, both online and offline. In a short span of time, the global value of BNPL transactions is projected to raise to $596.7 billion by 2026, as reported by (Krijnsen et al., 2023).

This rapid expansion of FinTech platforms, including BNPL services, has led to increased privacy concerns due to the extensive collection of sensitive user data that includes Personally Identifiable Information (PII) and Personal Financial Information (PFI), due to the nature of the service they provide. Existing research by (Dorfleitner & Hornuf, 2019) addresses the core data privacy issues prevailing within the Fintech industry. Their study involves identifying and understanding the risks evolved due to the way the data processed and handled by the Fintech companies. User data is collected by the companies majorly for credit assessment, fraud prevention, and marketing purposes. But the issue arises when there is an extensive collection of sensitive data from users for unknown purposes. Without proper security measures, these data are exposed to severe consumer privacy risks such as data breaches, unauthorized access, and identity theft. While (Hernández et al., 2019) identifies data privacy as the major concern due to the excessive collection of personally identifiable information (PII) data by Fintech firms

and the way it is handled exposing the consumer data to privacy risk resulting in cyber risks such as data breach and identity theft, (Hukum et al., 2021) highlights the practices of selling consumer data by Fintech companies to third parties and its subsequent consequences. To add up a real-world example, Klarna, one of the leading BNPL providers experienced a significant data breach affecting more than 90,000 users underlines the risk associated with these services.

In the case of BNPL industry, the luxury of buying things instantly with smaller payments have made customers to indulge in data sharing practices. As a result, the privacy aspect has taken a backseat leading to sensitive user data potentially being target of cyber-attacks and other privacy related risks. A Privacy risk Assessment, in practice is the most effective tool to manage these risks by introducing privacy by design concept into the system. Moreover, Article 35 of GDPR mandates the use of DPIA for businesses processing sensitive user information. Even though there is a promising privacy policy changes with the introduction of GDPR, (Zaeem & Barber, 2020) argues that companies still lack in transparency of how the PII data collected is processed and used.

2. Research Question:

How can Privacy Impact Assessment (PIA) framework be developed to effectively identify and mitigate data privacy in emerging BNPL services?

The privacy risks identified by many researchers in the Fintech industry with limited research on mitigation is the motivation for this research. A generalized solution is not effective to all industry types because risks are unique to each product or industry. The limitation of general applicability by existing PIA frameworks is covered in numerous academic literatures. Therefore, this research is conducted to pinpoint vulnerabilities and privacy risks specific to the widely adopted BNPL platform and provide relevant solutions to mitigate them by developing a Privacy Impact assessment tailored to the BNPL sector.

With successful completion of this research, the study aims to contribute to shape a standardised PIA framework adapted to the BNPL sector. The tailored PIA framework will include recommendations to enhance data privacy and data protection practices within the BNPL sector, thereby significantly protecting the consumer privacy by focusing on transparency, accountability, social and regulatory aspects in this digital ecosystem.

The remainder of this paper is organized by the following order. Section 2 reviews the existing research conducted on general and sector-specific PIA frameworks, comparison of existing frameworks and privacy enhancing technologies. Furthermore, Section 3 outlines the research methodology employed to conduct this study. Section 4 and 5 presents the design and implementation of the research respectively. Finally, Section 6 evaluates the proposed PIA framework tailored for BNPL sector.

3. Related Work

This section reviews prior research on Privacy Impact assessment frameworks and aims to identify the essential factors to consider while developing an effective PIA framework. By exploring related work, this study aims to identify gaps and opportunities for developing a PIA tailored to the BNPL sector. The relevant literature was gathered from sources such as Google scholar and IEEE Xplore. These platforms were chosen for their vast collection of peer-reviewed articles and academic books to maintain integrity of the sources. Initially, keywords like “privacy impact assessment”, “privacy and finance”, were used to identify related literature. Various filters like publication year, citation count and relevance were used to narrow down the results. Finally, the selected works were then grouped into categories and reviewed to understand patterns and gaps in the existing research, focusing on how they aligned with my research question.

3.1 Privacy Impact Assessment Research

3.1.1 Existing Privacy Impact Assessment Framework

Privacy Impact Assessment (PIA) is considered as an ideal method to assess the privacy aspect of a service or a product while focusing on data protection, as explored by Wright(Wright, 2012) . The concept of privacy is incomplete without integrating data protection into it. With an understanding of this foundational concept, (Timón López et al., 2021) recommended a two-layered Data Protection Impact Assessment (DPIA) methodology, built to achieve the concept of ‘privacy by design’. This concept introduces a proactive style of assessing privacy risk before the implementation of a product or a service. The proposed methodology consists of two stages: the former involves a pre-implementation analysis to identify privacy risks, evaluate potential impacts, and propose mitigation measures, while the latter involves assessing compliance with data protection regulations during the implementation. Building on structured methodologies, (Oetzel & Spiekermann, 2014) identified the shortcomings of the existing PIA practices introduced by (Wright) and presented a seven-layered privacy impact assessment method that focuses on ‘privacy by design’ based on the BSI risk practices. It includes a step-by-step process that includes defining system characteristics, identifying privacy targets and threats, evaluating the impact and the protection required, identifying mitigation measures, assessing residual risk, and documenting the PIA results to inform the stakeholders of the status and ensure compliance. In fact, this approach was introduced as a guideline by the German Federal Office for Information Security (BSI) on their RFID application.

Similarly focusing on integrating technology in privacy assessment,(Ahmadian et al., 2018) proposes a model-based approach to Privacy Impact Assessment aimed at improving upon the framework introduced by (Oetzel & Spiekermann, 2014). The proposed model utilises Unified Modelling Language (UML) security checks to identify privacy threats early in the system development process. The process mainly involves documenting system designs with privacy and security profiles, analysing privacy risks using an automated tool called CaRiSMA, and mapping identified threats to relevant controls and documenting results in a structured PIA report that aligns with GDPR requirements. Another study by (Bieker et al., 2016) identifies

Data Protection Impact Assessment (DPIA) as a critical tool for identifying and mitigating risks concerned with personal data processing. Taking on account the effect of GDPR which mandates the conduction of DPIAs for high-risk data processing systems, the authors suggest a three-step practical and systematic methodology to conduct DPIA's that aligns with the CIA (confidentiality, integrity, availability) triad and regulatory compliance. Apart from PIA methods from academic papers there are also other well-known policy driven papers, published from Data Protection Authorities from various countries such as the UK PIA Code of Practice(*Draft: Conducting Privacy Impact Assessments Code of Practice | Enhanced Reader*, n.d.), New Zealand PIA toolkit(*Office of the Privacy Commissioner | Privacy Impact Assessment Toolkit*, n.d.), Australian ICO PIA guide(*Guide to Undertaking Privacy Impact Assessments | OAIC*, n.d.) and CNIL PIA method(*Privacy Impact Assessment (PIA) | CNIL*, n.d.) and Canada directive on PIA(Secretariat, n.d.).

3.1.2 Sector-specific Privacy Impact Assessment

Sector-specific Privacy Impact Assessments are targeted to address privacy risks unique to certain industries. To begin with, (Tancock et al., 2010) introduced a Privacy Impact Assessment designed specifically to integrate with cloud solutions. The conceptual tool described by the authors have the potential to proactively enhance the privacy, compliance and mitigate associated risks within cloud environments, providing tailored guidance to the solution. Healthcare is one another sector where regulatory requirements mandate on conducting a PIA due to the nature of data this sector handles. (El Jaouhari & Bouabdallah, 2018) proposed a privacy safeguard framework for a healthcare architecture based on WebRTC (Web Real-Time Communication) with the Web of Things (WoT) to enable secure, real-time telemedicine services. The framework was developed by first analysing the privacy requirements, followed by identification of privacy leakage points, combined by GDPR regulations to conduct a privacy impact assessment, and proposing counter measures tailored to the e-health architecture. Although this framework provides a comprehensive coverage on sthe authors acknowledge shortcomings in integrating mitigating measures such as archiving, secure storage, data minimization and anonymity.

Similarly, in the healthcare domain, (Todde et al., 2020) proposed a DPIA methodology tailored to healthcare information systems, which utilized a modular approach focusing on individual system components instead of processing activities, thereby making it easier to integrate the DPIA when a new system is added. The authors tested this method on eleven software systems in a healthcare setting, revealing critical issues such as insufficient data security and authentication, which made the GDPR requirements fall short. Extending the application of tailored PIA approaches, (Henriksen-Bulmer et al., 2020)introduced the DPIA Data Wheel, a DPIA framework based on Contextual Integrity (CI), to facilitate PIAs tailored to Cyber Physical Systems (CPS), mainly focusing on charity organisations to comply with GDPR. The methodology presented involves aligning CI principles with GDPR and ICO guidance, using a series of questions to evaluate privacy risks and mitigation strategies that not only affects an organization but individuals alike. The results from this empirical study demonstrated its ability to identify nuanced privacy risk that would not be identified during a traditional privacy impact assessment and shifted the pre-conditioned perspective to consider risks from the individuals' point of view.

Furthermore, (Reuben et al., 2016) outlined a PIA template for provenance data in an application setting, focusing on protecting personal data from unintended disclosure. The authors outlined a four-step method applied to examples like loyalty and provenance graphs to identify specific privacy threats and mitigate them using GDPR principles. The key threats identified includes data minimization, function creep, inferred data processing, and obstacles to data access or deletion where provenance was available in open web and identified that there was an absence of mitigation measures for most of the threats identified which made the utility more vulnerable.

With the rising popularity of AI systems, (Ivanova, 2020) proposed a DPIA framework as a legal tool to prevent discriminatory practices and enforce equality in AI systems, one of the fundamental rights that GDPR aims to protect. The authors suggested a methodological framework focused on assessing and mitigating risks to bias, integrating GDPR principles such as fairness, accountability, and data minimization. The results highlighted that by upgrading, DPIA, it poses the potential to prevent algorithmic bias by ensuring fairness and transparency in AI systems. Finally, expanding the discussion to Identity Management Systems (IdM), (Timón López et al., 2021)explored the use of DPIA in a multi-layered approach to evaluate the degree of privacy by design in technological projects. The framework was deployed on a case study of the European OLYMPUS project, focusing on Identity Management (IdM) systems to identify privacy risks like password distribution risk and proposed improvements such as multi-factor authentication to enhance security and regulatory compliance. The author iterates the fact that that traditional DPIA process has its shortcomings especially to evaluate a technology that has not been implemented yet but can certainly be used to study the balance of the results achieved.

3.1.3 Overview

Privacy Impact Assessment have drastically evolved to accommodate privacy by design and regulatory compliance emphasizing on structured methodologies, proactive risk identification, and integration of technology to mitigate privacy risks effectively.

3.2 PIA Comparison Research

3.2.1 Evaluation of existing Privacy Impact Assessment

Several research were conducted to evaluate the efficiency of the existing PIAs by academic experts. For example, (Alshammari & Simpson, 2018) analysed two existing frameworks namely the CNIL and the PRIAM framework. CNIL Methodology defines to be a risk model utilizes a semi-quantitative approach focusing on potential threats, incidents, vulnerabilities, and risk sources while PRIAM employs a combination of qualitative and quantitative assessment to specify key risk factors on privacy impact and potential threats evaluation. However, the author criticises both the frameworks for limited capabilities of risk sources and their inability to categorize certain risks and their impacts accurately and identifies them to be overly generic that pose challenges to apply to all industries. To address these issues, the author suggests for an expanded privacy risk model that integrates technical, legal, ethical, and organizational aspects to systematically identify, analyse, and prioritise privacy risk to ensure an effective assessment process.

Similarly, expanding the scope of evaluation, (Bisztray & Gruschka, 2019) assess the effectiveness of three popular PIA methods, selected as academic, policy -driven and international namely LINDDUN, CNIL, and ISO/IEC 29134:2017, based on their practicality and compliance with GDPR requirements. Interestingly, the study concluded that none of the frameworks were able to meet all criteria. For instance, while LINDDUM focuses on privacy threats, it lacks a risk assessment component. Meanwhile, CNIL framework is compliance focused but lacks integration of process. On the other hand, ISO/IEC 29134 provides the most comprehensive guidance; however, its repetitive nature and general applicability, limits it effect on sector-specific applications where unique privacy risks arises. Therefore, the author recommends developing improved or sector specific DPIA frameworks to better address privacy and data protection challenges.

To conclude, (Vemou & Karyda, 2020) evaluates nine widely used PIA methods and evaluates them by identifying best practices from privacy literature. Moreover, the study identifies critical gaps and differences in existing PIA framework that includes lack of practical guidance for implementation, limited tools to automate risk assessment processes, insufficient insight on the assignment of roles and responsibilities and stakeholder engagement. The author concludes that optimizing PIA methods requires addressing the gap for improved templates along with more tailored guidance for specific industries or technologies.

3.2.2 Overview

Most of the existing Privacy Impact Assessment methods are built for general applicability and lacks effectiveness to identify unique risks pertaining to specific industries. To address this gap, the authors collectively recommend developing tailored PIA models to better address privacy challenges.

3.3 Privacy Enabling Technology Research

3.3.1 Why use PET?

Privacy enabling technology (PET) is defined by European Union Agency for Cybersecurity (ENISA) as "*Software and hardware solutions, i.e. systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons*" (*How Can PETs Help with Data Protection Compliance? | ICO*, n.d.). With an extensive handling of PII data by financial institutions, it is more of a necessity to integrate PET into the system. To support this, Yun and Siani(Yun Shen, n.d.) analyses Privacy Enabling Technologies from various domains such as anonymization, identity management, data processing, policy checking, and network protection to determine their contribution to significantly minimise privacy threats. The authors emphasize that privacy is contextual, and the selection of PETs must align with specific business and regulatory needs, which can be achieved only by conduct a PIA. Moreover, the study highlights that the adoption of PET in an organization requires comprehensive privacy risks assessment, budget, and its usability. With an influx in the adoption of AI systems in financial systems, Khanh (Khanh Nguyen, n.d.) discusses significant data privacy concerns such as the lack of transparency, consent, and ethical handling of data in AI systems and suggests the use of PETs like differential privacy, federated learning, and secure multi-party computation to protect privacy while enabling AI functionality.

Furthermore, experts(Baum et al., 2023) identifies the key privacy challenges faced by financial systems connecting to protect identities and transaction values to ensure compliance with legal and regulatory requirements. The author identifies the application of PETs and categorizes them systematically to address the privacy challenges outlined before. Also, researchers(Li et al., 2024) emphasizes the importance of integrating PETs in financial intelligence to support the balance between data privacy and effective financial crime detection.

3.3.2 Overview

Privacy enabling technologies play a critical role in protecting privacy, particularly in financial systems handling sensitive data and underscores the importance of PIA and tailored PETs to balance privacy with compliance and functionality.

4. Research Methodology

The research methodology employs a systematic approach to ensure an optimal result in the development of a PIA framework, as discussed in the research literature(Bieker et al., 2016; Oetzel & Spiekermann, 2014; Timón López et al., 2021). This methodology consists of five key layers: data collection, data flow analysis, risk assessment, PIA development and evaluation as illustrated in Fig.1. The main purpose of this research is to develop a tailored PIA framework to identify and mitigate privacy risks specific to the BNPL industry.

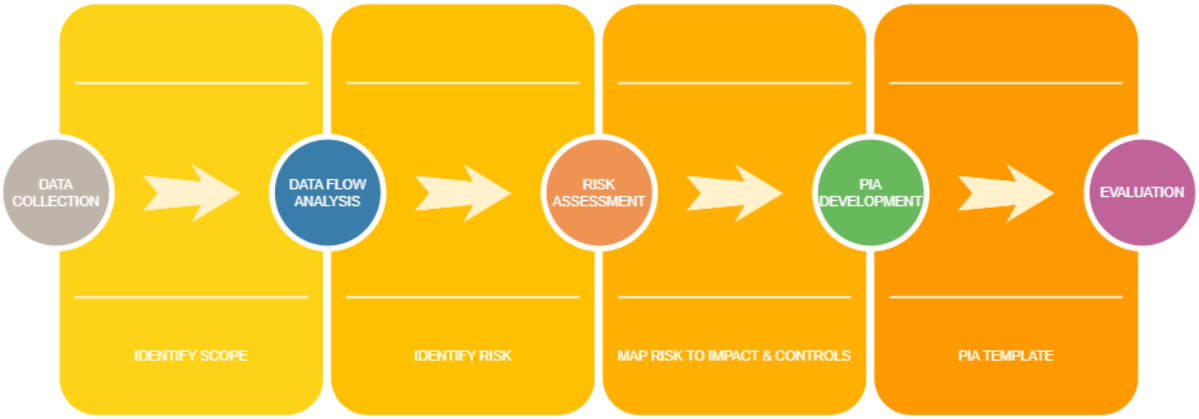

Figure 1. Overview of research methodology

The primary source of data for the research conducted are privacy policies of BNPL providers in Ireland. A study specifically on the Ireland region was conducted so that research is localized to a particular region to be more effective before applying the results globally.

For mapping the data flow analysis, a custom-made data mining tool tailored to the BNPL sector was built to make the analysis easier. Even though the tool Privacy Check build by (Zaeem & Barber, 2021)was publicly available to use, it was no more supported by Google chrome as an extension. Therefore, a custom tool was built to summarize and classify privacy policies to pre-defined categorized tailored to BNPL industry.

For risk assessment, identified privacy risks are mapped to the likelihood of occurrence and its potential impact. This method was widely used in various sectors successfully (El Jaouhari & Bouabdallah, 2018; Henriksen-Bulmer et al., 2020; Todde et al., 2020)to identify and prioritize risk to identify control measures.

For PIA development, standard DPIA templates and guides were followed to ensure standardization of the framework and adaptability of the report for a broader audience.

For evaluation, PEGS (Privacy Evaluation and Grading System) (Wadhwa & Rodrigues, 2013) method was chosen due to its credibility. This method was the result of research undertaken in the Privacy Impact Assessment Framework for Data Protection and Innovation: The European Journal of Social Science Research 177 Privacy Rights (PIAF) project, funded by the European Commission's Directorate-General Justice to enhance the effectiveness of a PIA.

5. Design Specifications

The Privacy Impact Assessment (PIA) framework serves as the basis for identifying, analysing, and mitigating privacy risks associated with he Buy Now, Pay Later (BNPL) providers. This framework illustrated in Fig 2. has been designed by integrating key components, procedures and metrics identified from the academic literature, for a thorough assessment.

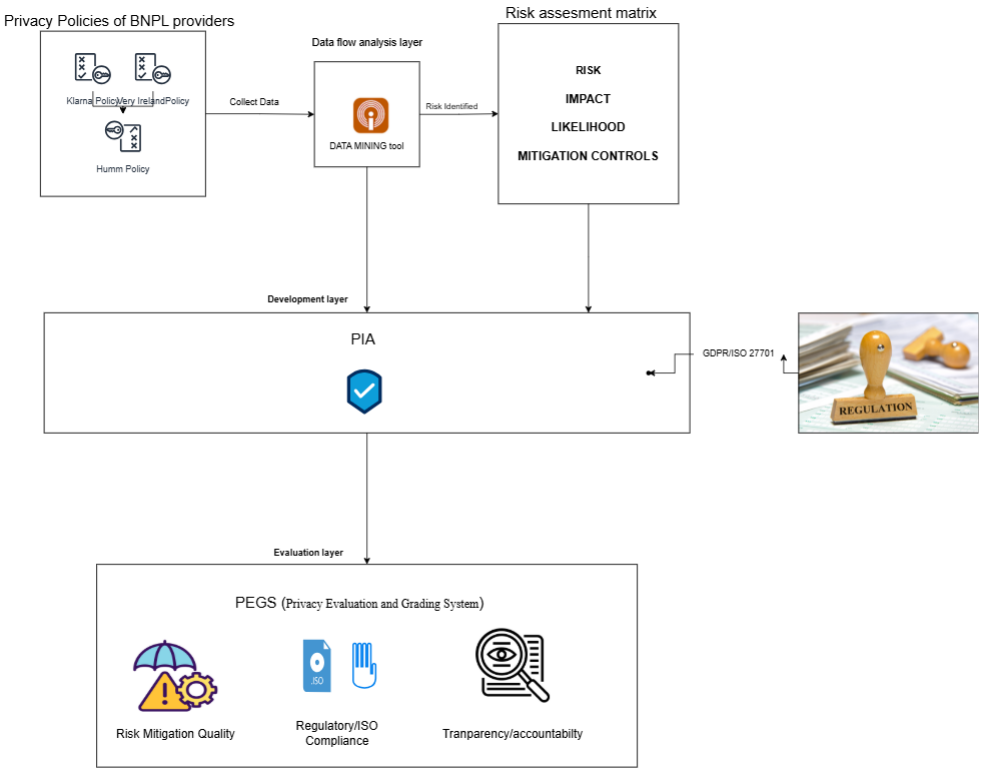

Figure 2. Framework development architecture

5.1 Key Components of the Framework

1. *Privacy Policies*:

The initial step of the framework is to gather privacy policies of the BNPL providers, predominantly in Ireland. These policies are the primary source of data, and gives the nature of the providers data collection, sharing, usage, and retention practices. The results of analysing these policies will give us an insight into the privacy risk landscape of the BNPL industry and helps in defining the scope of the assessment.

2. *Data flow analysis*:

Once the privacy policies are sourced, the next step of the framework is to analyse and understand how user data flows within the BNPL ecosystem. This includes identifying how data is collected, where it is stored, how it is processed, and how and whom the data is shared with. For this purpose, a custom data mining tool that utilizes machine learning was developed to speed up the analysis process.

Data mining tool design:

The data mining tool is designed to perform the following functions:

i. Extraction and Summarization: Privacy policies are often lengthy and filled with legal contents. By extracting and summarizing, the tool aims to provide the user with a concise overview of the policy content.
ii. Categorized content: Categorizes are predefined in the context of BNPL services such as Data Collection, Data retention, Data sharing, Security measures, User rights, and General information. Each of the sentences of the privacy policies are categorized automatically by this tool, making the analysis process easier. This helps in breaking down the policies into meaningful sections. This helps in identifying how data flow within the BNPL system.
iii. Visualization: By visualizing the categorized content, the tool aims to highlight areas of focus in the privacy policy.

Tools used:

i. Python Libraries – used to handle input-output functions.
ii. SpaCy - used to process large volumes of unstructured text using Natural Processing Language (NLP)
iii. Hugging face transformers – used Pre-trained ML models like facebook/bart-large-cnn to specialized for tasks like summarization.
iv. Scikit-learn - Scikit-learn is used to classify sentences to predefined privacy domains. It was used to import TfidfVectorizer for converting text into numerical vectors and Cosine-similarity for measuring the similarity between sentence_vectors and category_vectors to predict the category of the sentence.

3. *Risk Assessment Matrix*:

The critical component of this framework is the risk assessment matrix to evaluate identified risks and helps in prioritisation of mitigation measures where high priority risk receives immediate resolution. Since the threat landscape evolves with new emerging threats, it is

essential to repeat this process regularly. The matrix categorizes risks based on three parameters:

- Likelihood: The probability of the risk occurring. The likelihood score is set from 1-5 where score of 1 is described as "Very Unlikely" with a probability of occurrence of less than 10%; 2 as "Unlikely" with a probability of occurrence between 10% and 30%, 3 as "Possible" with a probability of occurrence between 31% and 50%, 4 as "Likely" with a probability of occurrence between 51% and 70%, 5 as "Very Likely" with a probability of occurrence of more than 70%. These scores are determined by analysing historical data like frequency of similar risks.
- Impact: The severity of the risk if it occurs and is scored between 1-5. where score of 1 is assigned as "Negligible" with a minimal impact, 2 as "Minor" with a small impact, 3 as "Moderate" with a noticeable impact, 4 as "Major" with a significant impact and 5 as "Critical" with catastrophic impact. These scores are determined based on factors such as regulatory fines, reputational damage, financial loss and consumer trust degradation.
- Risk Score: Risk score is calculated by multiplying the likelihood and impact score. Risk that scores between 1-6 are considered low, 7-15 as medium and 16-25 as high-risk categories.
- Mitigation Strategies: Actions to minimize or prevent the risk. The mitigation controls are aligned to ISO/IEC 27701 privacy controls which is the international standard for privacy management in order to standardize the framework.

4. Development of PIA:

Using the insights of data flow analysis and risk assessment matrix unique to the BNPL sector, a PIA template is developed leveraging the regulatory requirements of (GDPR/ISO) and the existing general DPIA template. This step involves designing a PIA template adaptable to various BNPL providers. It documents identified risks, mitigation strategies, compliance measures, ensuring transparency for users and usability for stakeholders.

5. Evaluation:

Finally, to evaluate the effectiveness of the PIA developed, the framework incorporates PEGS (Privacy Evaluation and Grading System) (Wadhwa & Rodrigues, 2013)method based on 10 criteria's that covers the metrics such as:

- Regulatory Compliance – Adherence to GDPR and ISO standards.
- Risk Mitigation – Effectiveness of proposed strategies to reduce identified risks.
- Transparency – Transparency and clarity of the PIA documentation.
- Accountability – Assignment of roles and responsibilities for tracking implementation.

5. Implementation

5.1 Data Collection

The source data was collected from three major BNPL providers in Ireland: Klarna, Very Ireland and Humm, assigned as P1, P2, P3 respectively for analysis purposes. These policies are gathered from the official websites of the respective BNPL providers. The structure of these

policies follows a standard format containing sections such as introduction to data protection practices, list of data controllers, detailed section of data collection and usage, legal basis for processing the data collected, data retention policies, user rights, data sharing practices, fraud prevention measures, and contact details for inquires and complaints. These policies give us a comprehensive insight on what kind of data is collected or processed, including whether it involves sensitive information like Personally Identifiable Information (PII) or Personal Financial Information (PFI) data, the purposes for collecting the data, the security measures placed to protect the data against privacy threats, user rights and more.

5.2 Data Flow analysis

Once the data required is sourced, a custom-built data mining tool that utilises machine learning is deployed to understand the lifecycle of user data within the BNPL ecosystem. This stage identifies how the user data is collected, processed, stored, and shared, providing knowledge about the potential privacy risks and vulnerabilities. The sourced privacy policies were converted to a text format to feed into the tool for analysis. The tool preprocesses text of the privacy policies to extract key contents and summarizes the lengthy text into concise content for efficient analysis. For example, the privacy policy of Very Ireland was summarized from a lengthy 2500 words file to approximately 500 words as depicted in Fig 4.

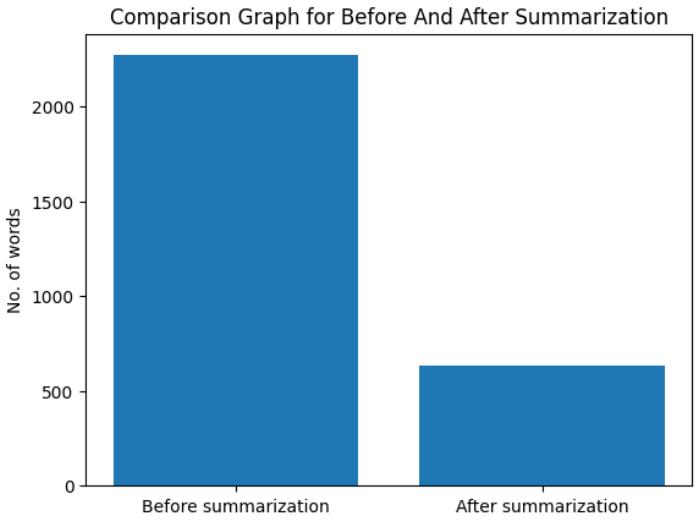

Figure 4. Comparison of Very Ireland before and after summarization

Next on, the tool automatically categorizes each sentence of the inputted privacy policies into pre-defined categories that complement our analysis in the context of BNPL sector. The sentences are classified into one of the predefined privacy domains:

- Data Collection – Identifies how user data is gathered, including PII, PFI data.
- Data Sharing – Identifies the sharing of user data with third parties such as service providers, regulatory authorities.
- Data Retention – Identifies the duration of the data stored, archiving and deletion policies.

- User Rights – Identifies the user's ability to access, modify or delete their data, and opt-out of specific data processing activities like marketing purposes.
- Security Measures – Identifies the security mechanism in place to protect the user data that includes encryption, fraud detection, anonymization and much more.
- General Information – Identities data that doesn't fit into other categorizes.

```
Sentence: What Data we Process and Share
The personal data you have provided, we have collected from you, or we have received from third parties may include your:

name

date of birth

nationality (only where you have had to supplement ID)

gender (only where you have had to supplement ID)

residential address and address history (only where you have had to supplement ID/apply for credit with SDI)

contact details such as email address and telephone numbers

financial information (only where you apply for credit with SDI)

employment details (only where you apply for credit with SDI)

identifiers assigned to your computer or other internet connected device including your Internet Protocol (IP) address

Eircodes (required to enable us deliver good to you as quickly and accurately as possible)

When we and fraud prevention agencies process your personal data, we do so on the basis that we have a legitimate interest
Predicted Label: Data collection
```

Figure 6. Categorized content of policy

The distribution of the contents into these categorizes as shown in Fig 6. makes the process of analysis easier and helps in mapping the data movement while highlight areas of concern, such as potential over-collection or unauthorized sharing of sensitive data. The distribution of sentences was then visualized as shown in Fig 7. for better understanding of the areas to focus on.

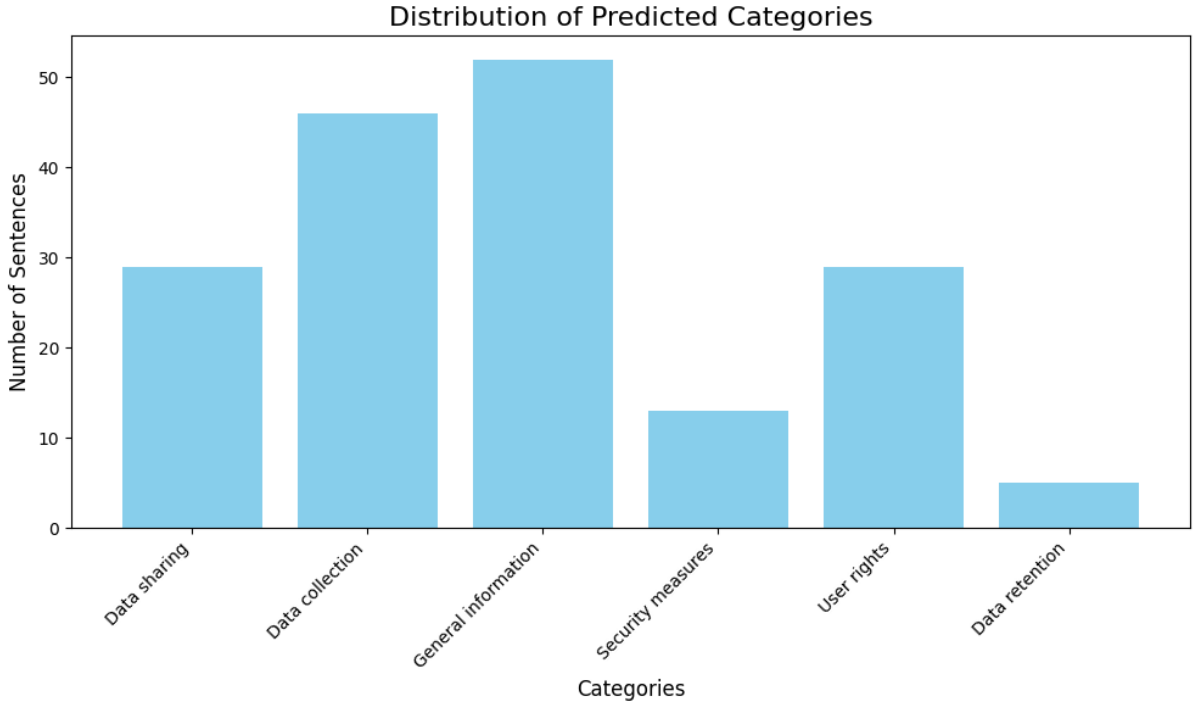

Figure 7. Distribution of Predicted Categories

By analysing the policies of P1, P2, and7 P3, specific vulnerabilities as described in Table 1. associated with extensive data collection, third-party risks, cross-border transfers, automated decision making, unclear data retention policies, user rights accessibility, marketing practices were identified that may arise as potential data and privacy risks.

Risk	P1 (Klarna)	P2 (Very Ireland)	P3 (Humm)	Conclusion
Extensive Data Collection	Collects PII, biometric data, financial and device data.	Captures employment history, browsing activity, and PII.	Collects financial details, employment data, and PII.	All providers collect significant personal and financial data.
Third-Party Data Sharing	Shares data with merchants, financial institutions, and fraud prevention agencies.	Shares data with marketing partners and service providers.	Shares data with insurers, credit bureaus, and service providers.	Broad sharing practices indicate potential misuse risks.
International Data Transfers	Transfers data globally, including non-EEA countries.	Transfers data to the UK and international locations.	Transfers data to regions like the Philippines and Australia.	Cross-border transfers pose compliance and security risks.
Automated Decision-Making	Utilizes automated systems for fraud and credit evaluations.	Automates credit checks and fraud assessments.	Relies on automated processes for credit decisions.	Transparency and fairness in decision-making remain a challenge.
Unclear Data Retention Policies	Lacks specific retention periods for different data types.	Retains data for up to 7 years but lacks differentiation by data type.	Does not define retention timelines clearly.	Vague retention policies leads to risks of prolonged data storage and misuse.
User Rights Accessibility	Users must initiate actions to access or delete data.	Provides rights but could streamline processes.	Accessibility of user rights is somewhat burdensome.	User difficulties in accessing rights are consistent across providers.
Data Security and Encryption	Mentions encryption and pseudonymization but lacks technical details.	Mentions security measures but provides insufficient details.	Mentions encryption and data anonymization but lacks specifics.	Insufficient disclosure of security protocols highlights potential vulnerabilities.

Direct Marketing Practices	Relies heavily on legitimate interest for marketing without explicit opt-ins.	Uses consent for marketing but with unclear opt-in processes.	Practices rely on user consent but may not be fully explicit.	Marketing practices may lack balance with user rights.

Table 1. Identified Risk

The identified risks help in the next stage of risk assessment process.

5.3 Risk Assessment

During the risk assessment process, the privacy risks aligned during data flow analysis were evaluated systematically which classifies risk based three main factors such as likelihood, impact, and overall risk score. This ensures tailored mitigation strategies aligned with the regulatory and operational requirements of the BNPL sector, especially within the ISO/IEC 27701 privacy framework. The output of the risk assessment stage is depicted in Table 2. This matrix gives a comprehensive understanding of the risks associated with BNPL sector, their priority levels, responses to the risks making it critical component for managing and mitigating risks effectively.

Risk	**Description**	**Likelihood**	**Impact**	**Risk Score**	**Mitigation Strategies**
Extensive Data Collection	Collecting excessive PII and PFI data.	4 (Likely)	5 (Critical)	20 (High)	Implement data minimization; collect only essential data.
Third-Party Data Sharing	Sharing user data with partners and agencies.	3 (Possible)	4 (Major)	12 (Medium)	Enforce strict data-sharing agreements and monitor GDPR compliance.
International Data Transfers	Transferring data to non-EEA countries.	3 (Possible)	4 (Major)	12 (Medium)	Encrypt data before transfer; review SCCs regularly.
Automated Decision-Making	Limited manual review of credit/fraud decisions.	3 (Possible)	4 (Major)	12 (Medium)	Provide manual review options and transparency in algorithms.
Unclear Data Retention Policies	Prolonged storage of sensitive data.	2 (Unlikely)	3 (Moderate)	6 (Low)	Define clear retention timelines;

					automate deletion.
User Rights Accessibility	Difficulty accessing or modifying personal data.	3 (Possible)	3 (Moderate)	9 (Medium)	Develop user-friendly portals for managing data rights.
Data Security and Encryption	Insufficient information on security controls.	3 (Possible)	4 (Major)	12 (Medium)	Implement robust encryption; conduct regular penetration testing.

Table 2. Risk assessment Matrix

The mitigation strategies listed above are specifically mapped to ISO/IEC 27701 controls as stated below:

A.7.2.1: Data minimization.

A.7.2.2: Purpose specification and limitation.

A.7.2.3: Fair and lawful processing.

A.7.2.4: PII quality and accuracy.

A.8.2.2: Minimization of PII collection.

A.8.2.3: Retention management.

A.7.3.3: Compliance with legal requirements.

A.7.4.1: PII principals' rights.

A.7.4.2: Mechanisms for exercising rights.
measures.

A.7.5.1: Sharing, transfer, and disclosure.

A.7.5.2: Third-party agreements.

A.7.6.1: Transparency of processing.

A.8.1.2: Providing PII access.

A.8.3.1: PII retention policies.

A.8.3.2: Deletion and disposal of PII.

A.8.4.1: Secure transfer of PII.

A.8.5.3: International transfer of PII.

A.10.1.2: Encryption during transfer.

A.10.1.3: Technical and organizational security

5.4 PIA Development

A tailored PIA template is developed to ensure it aligns with unique characteristics and privacy risks associated with the Buy Now Pay Later (BNPL) sector. By incorporating the outputs attained from data flow analysis and risk assessment from the previous stages, a tailored PIA template was derived from an established general DPIA template, to ensure compatibility with general DPIA methodologies while adhering to regulatory standards, including GDPR and ISO/IEC 27701. The developed PIA framework comprises of several critical components to ensure comprehensive privacy risk assessment and mitigation as follows:

i. System Overview – detailed description of the BNPL provider's system, including its purpose, scope, and data processing activities. It also identifies the roles of data

controllers and processors, to provide clarity on the responsibilities within the data cycle.

ii. Data Overview – Maps the data collected such PII and PFI, identifies data sources, processing activities, and purpose of use.

iii. Risk Identification and Mitigation – Risk assessment of the privacy risks identified such as data collection, automated decision making, data sharing practices, data retention and data security practices. Tailored mitigation measures are proposed for each risk, including measures like data minimisation, encryption, use of SCCs, pseudonymization, AI- resilient security frameworks and much more.

iv. Privacy Rights and Accountability – clear guidance on user rights, including access, modification, deletion, and opt-out options of specific data processing activities. Also, specific accountability roles to ensure compliance and implementation throughout the PIA lifecycle.

v. Evaluation metrics: Post-implementation evaluation metrics like regulatory compliance, risk mitigation quality and transparency audits are included to assess the effectiveness of the proposed mitigation strategies and to ensure compliance with regulatory requirements like the GDPR.

vi. User Friendliness – The PIA template is structured in a questionnaire format, providing clear guidance to the stakeholders across legal, technical and processes domain. This ensures the PIA is easy to understand and use by any users without previous experience as well.

6. Evaluation

The effectiveness of the PIA developed is evaluated using the the PEGS (Privacy Evaluation and Grading System) approach as described in the Wadhwa and Rodrigues paper and the template was systematically assessed across the PEGS criteria.

6.1 Evaluation Criteria and Compliance Justification

1. Early Initiation

The PIA template contains sections to document the system overview and data lifecycle early in the project. This meets the requirement for initiating PIA early enough to influence design decisions to make it privacy by design.

2. Identification of who conducted the PIA

The template includes fields for organizations name, PIA unique identifier, and responsible stakeholders such as data controllers and processors. This allows clear identification of the entity that conducts the PIA.

3. Project Description, Purpose, and Context

The template requires a description of the system, purpose, and the types of data collected, which gives an overall understanding of the scope of the PIA.

4. Information flow mapping

There is clear guidance to map data collection, processing, storing, and sharing practices that satisfies this criterion.

5. Legislative Compliance Checks

The template includes a section to ensure alignment with legal frameworks such as GDPR and ISO/IEC 27701.

6. Identification of Privacy Risks and Impacts

Unique privacy risks related to data collection, automated decision-making, data sharing, security are addressed in detail. Each risk is mapped to relevant mitigation measures.

7. Identification of Solutions/Options for Risk Avoidance and Mitigation

The template provides effective mitigation strategies aligned with ISO standards and other regulatory frameworks such as GDPR.

8. Recommendations

Recommendations are integrated into timeline and allows their implementation timelines.

9. Publication

The template lets documentation visibility to stakeholders, fulfilling the transparency requirements.

10. Stakeholder consultation

The template includes fields for documenting stakeholder engagement throughput the PIA lifecycle.

The above criteria are graded using the PEGS grade chart shown in Table 4. The result of the evaluation score of the PIA report justified is shown in Table 4., which scores a fully compliant criteria with a score of 8, partly complaint criteria with a score of 5 and the ones that do not comply with a score of 2. The weight of the criteria is divided into three categories: the basic criteria that weighs 1 are considered least-important such organization name, initiation stage , publication but is still valuable since missing out these criteria will lead to the failure of early identification of design changes; the criteria that weighs 2 are process focused such as compliance and data flow analysis, are important to check the transparency and accountability of the PIA report; and the criteria that weighs 3 are the most essential ones like the risk mitigation quality that are critical for an effective PIA report.

	Grade chart	
Excellent	141 - 160	A+
Very good	121 - 140	A-
Good	101-120	B+
Acceptable	81-100	B-
Inadequate/requires improvement	61-80	C
Failure	40-60	D

Table 3: Grade chart of PEGS

Evaluation criteria for PIA reports	Criteria weight	Proposed PIA
Clarification of early initiation	1	8
Identification of who conducted PIA	1	8
Project description, purpose and relevant contextual information	2	16
Information flow mapping	2	16
Legislative compliance checks	2	16
Identification of privacy risks and impacts	3	24
Identification of solutions/options for risk, avoidance, mitigation	3	24
Recommendations	3	24
Publication	1	8
Identification of stakeholder consultation	2	16
Score		160
Grade		A+

Table 4. Evaluation result

As per the results of the PEGS Evaluation score, the PIA tailored for the BNPL sector scores a perfect score of 160, demonstrating excellent alignment with PEGS evaluation criteria, thereby effective to mitigate potential privacy risks identified in the BNPL sector.

7. Conclusion and Future Work

The Privacy Impact Assessment (PIA) framework tailored for the Buy Now, Pay Later (BNPL) sector was successfully developed to address privacy risks unique to this industry by using systematic methodologies and tools. The framework integrates privacy-by-design principles with ISO/IEC 27701 privacy controls to ensure compliance with global standards and regulations like GDPR. Unique challenges of data privacy within BNPL services, including extensive data collection, third-party sharing, cross-border data transfers, and automated decision-making processes was identified. The risk assessment matrix effectively prioritizes these risks, enabling targeted mitigation solutions. The study demonstrated the value of using AI/ML tools, for analysing privacy policies easily. The PEGS evaluation highlights the effectiveness of the framework to protect privacy implications.

While this research focuses on presenting an effective PIA framework for the BNPL sector, the limitations include absence of quantitative analysis to measure the effect of privacy mitigation quality post implementation. The future work of this research will focus on engaging stakeholders for user awareness and participation in the PIA process for enhancing transparency and accountability. We could also extend the research to integrate monitoring measures for continuously evaluating the risk factor as new threats and regulations evolve, as this research focuses only on mitigation strategies.

References

Ahmadian, A. S., Strüber, D., Riediger, V., & Jürjens, J. (2018). Supporting privacy impact assessment by model-based privacy analysis. *Proceedings of the ACM Symposium on Applied Computing*, 1467–1474. https://doi.org/10.1145/3167132.3167288

Alshammari, M., & Simpson, A. (2018). Towards an effective privacy impact and risk assessment methodology: Risk assessment. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11033 LNCS*, 85–99. https://doi.org/10.1007/978-3-319-98385-1_7/FIGURES/3

Baum, C., Chiang, J. H., David, B., & Frederiksen, T. K. (2023). SoK: Privacy-Enhancing Technologies in Finance. *Cryptology EPrint Archive*. https://eprint.iacr.org/2023/122

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A process for data protection impact assessment under the European General Data Protection Regulation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9857 LNCS*, 21–37. https://doi.org/10.1007/978-3-319-44760-5_2/FIGURES/3

Bisztray, T., & Gruschka, N. (2019). Privacy impact assessment: Comparing methodologies with a focus on practicality. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11875 LNCS*, 3–19. https://doi.org/10.1007/978-3-030-35055-0_1

Dorfleitner, G., & Hornuf, L. (2019). FinTech and data privacy in Germany: An empirical analysis with policy recommendations. *FinTech and Data Privacy in Germany: An Empirical Analysis with Policy Recommendations*, 1–121. https://doi.org/10.1007/978-3-030-31335-7

Draft: Conducting privacy impact assessments code of practice | Enhanced Reader. (n.d.).

El Jaouhari, S., & Bouabdallah, A. (2018). A Privacy Safeguard Framework for a WebRTC/WoT-Based Healthcare Architecture. *Proceedings - International Computer Software and Applications Conference*, *2*, 468–473. https://doi.org/10.1109/COMPSAC.2018.10278

Guide to undertaking privacy impact assessments | OAIC. (n.d.). Retrieved December 8, 2024, from https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments

Henriksen-Bulmer, J., Faily, S., & Jeary, S. (2020). DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems. *Future Internet 2020, Vol. 12, Page 93*, *12*(5), 93. https://doi.org/10.3390/FI12050093

Hernández, E., Öztürk, M., Sittón, I., & Rodríguez, S. (2019). Data protection on fintech platforms. *Communications in Computer and Information Science*, *1047*, 223–233. https://doi.org/10.1007/978-3-030-24299-2_19/FIGURES/2

How can PETs help with data protection compliance? | ICO. (n.d.). Retrieved December 8, 2024, from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/how-can-pets-help-with-data-protection-compliance/#what

Hukum, P., Konsumen, B., Data, Y., Diperjual, P., Di, B., Magister, J., Nababan, R., & Sinaga, N. P. (2021). PERLINDUNGAN HUKUM BAGI KONSUMEN YANG DATA PRIBADINYA DIPERJUAL BELIKAN DI APLIKASI FINTECH PEER-TO-PEER LENDING. *Nommensen Journal of Legal Opinion*, *2*(02), 156–167. https://doi.org/10.51622/NJLO.V2I02.366

Ivanova, Y. (2020). The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12121 LNCS*, 3–24. https://doi.org/10.1007/978-3-030-55196-4_1

Khanh Nguyen. (n.d.). *Enhancing Data Privacy in Artificial Intelligence*.

Krijnsen, E., Crijns, J., & Sprenger, B. (2023). *Embedded finance: Challenging common assumptions*. https://www.pwc.com/gx/en/industries/financial-services/publications/embedded-finance-challenging-common-assumptions.html

Li, Y., Ranbaduge, T., & Ng, K. S. (2024). *Privacy Technologies for Financial Intelligence*. https://arxiv.org/abs/2408.09935v1

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems*, *23*(2), 126–150. https://doi.org/10.1057/EJIS.2013.18

Office of the Privacy Commissioner | Privacy Impact Assessment Toolkit. (n.d.). Retrieved December 8, 2024, from https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-toolkit/

Privacy Impact Assessment (PIA) | CNIL. (n.d.). Retrieved December 8, 2024, from https://www.cnil.fr/en/privacy-impact-assessment-pia

Reuben, J., Martucci, L. A., Fischer-Hübner, S., Packer, H. S., Hedbom, H., & Moreau, L. (2016). Privacy impact assessment template for provenance. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 653–660. https://doi.org/10.1109/ARES.2016.95

Secretariat, T. B. of C. (n.d.). *Archived [2021-04-01] - Interim Directive on Privacy Impact Assessment*.

Tan, G. K. S. (2022). Buy what you want, today! Platform ecologies of "buy now, pay later" services in Singapore. *Transactions of the Institute of British Geographers*, *47*(4), 912–926. https://doi.org/10.1111/TRAN.12539

Tancock, D., Pearson, S., & Charlesworth, A. (2010). A privacy impact assessment tool for cloud computing. *Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*, 667–676. https://doi.org/10.1109/CLOUDCOM.2010.27

Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). 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. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3469207

Todde, M., Beltrame, M., Marceglia, S., & Spagno, C. (2020). Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. *Informatics in Medicine Unlocked*, *19*, 100361. https://doi.org/10.1016/J.IMU.2020.100361

Vemou, K., & Karyda, M. (2020). Evaluating privacy impact assessment methods: guidelines and best practice. *Information and Computer Security*, *28*(1), 35–53. https://doi.org/10.1108/ICS-04-2019-0047/FULL/PDF

Wadhwa, K., & Rodrigues, R. (2013). Evaluating privacy impact assessments. *Innovation: The European Journal of Social Science Research*, *26*(1–2), 161–180. https://doi.org/10.1080/13511610.2013.761748

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review*, *28*(1), 54–61. https://doi.org/10.1016/J.CLSR.2011.11.007

Yun Shen, S. P. (n.d.). *Privacy Enhancing Technologies: A Review | Enhanced Reader*.

Zaeem, R. N., & Barber, K. S. (2020). The Effect of the GDPR on Privacy Policies. *ACM Transactions on Management Information Systems (TMIS)*, *12*(1). https://doi.org/10.1145/3389685

Zaeem, R. N., & Barber, K. S. (2021). The Effect of the GDPR on Privacy Policies. *ACM Transactions on Management Information Systems*, *12*(1). https://doi.org/10.1145/3389685

10. Appendix

10.1 Proposed BNPL PIA TEMPLATE

Privacy Impact Assessment (PIA) for [BNPL Service Name]

Date Signed:

[Insert Date]

Organization Name:

[BNPL Provider Name]

PIA Unique Identifier:

[P-XXXXXXXX-XXXXXX]

Section 1: System Overview

1.1 Name of the System:

[Name of the BNPL System/Platform]

1.2 Description of the System:

Provide a description of the BNPL system, its purpose, and how it operates.

1.3 Purpose of the System:

- What is the primary purpose of the system?
- Is there any secondary use of the collected data?
- Are users informed about both primary and secondary uses?

Section 2: Data Overview

2.1 Categories of Data Collected:

- What types of personal, financial, and behavioural data are being collected?
- Is the data being collected adequate, relevant, and limited to what is necessary for its intended purpose?

2.2 Sources of Data:

- From whom is the data collected (e.g., customers, merchants, credit agencies)?
- Are individuals notified about the data collection?

2.3 Data Processing Activities:

- What specific activities are carried out with the collected data (e.g., credit assessment, profiling)?
- Are these activities automated, and do they involve decisions impacting individuals?

Section 3: Privacy Risks and Mitigations

3.1 Data Collection

- Is the data being collected necessary for the intended purpose?
- Are users provided with clear and accessible information about what data is collected and why?
- Could over-collection of data lead to reputational or legal risks?

Mitigation Measures:

- Implement purpose limitation principles.
- Regularly review data collection practices to ensure compliance.

3.2 Automated Decision-Making

- Are users informed about decisions made through automated processes?
- Do users have the option to contest or seek human review of automated decisions?

Mitigation Measures:

- Provide transparency about automated processes.
- Allow opt-out or appeal mechanisms for significant decisions.
- Develop algorithms adhering to fairness and accountability standards.

3.3 Data Sharing and Transfers

- With whom is the data shared, and for what purposes?
- Do these parties comply with equivalent data protection standards?
- Are cross-border transfers compliant with regulations (e.g., SCCs, Privacy Shield, or equivalent)?

Mitigation Measures:

- Limit data sharing to necessary purposes.
- Conduct vendor risk assessments and ensure contractual safeguards.
- Encrypt data before international transfers.

3.4 Data Retention

- How long is the data retained, and is it necessary for its intended purpose?
- Are data retention periods clearly communicated to users?

Mitigation Measures:

- Implement retention schedules and automated data deletion mechanisms.
- Regularly review retention policies to ensure relevance.

3.5 Data Security

- Are sufficient technical and organizational measures in place to prevent breaches?
- Are pseudonymization, encryption, and AI-resilient security frameworks implemented?

Mitigation Measures:

- Encrypt data both in transit and at rest using advanced standards.
- Employ AI-resilient systems to detect and prevent security threats.

Section 4: Legal and Compliance Framework

4.1 Legal Authorities Governing Data Use:

- Are the data processing activities aligned with applicable legal frameworks (e.g., GDPR, ISO/IEC 27701)?
- Are there specific laws regulating BNPL services in the jurisdictions where the company operates?

4.2 Consent Management:

- Are users provided with clear choices to give or withdraw consent?
- How is consent documented and managed over time?

Section 5: Data Management and Security

5.1 Methods for Securing Data:

- What encryption standards and technical safeguards are in place to protect sensitive data?
- Are administrative safeguards (e.g., access controls) implemented effectively?

5.2 Access Controls:

- Who has access to data, and is access granted on a need-to-know basis?
- Are access logs maintained and reviewed periodically?

5.3 Retention and Destruction Policy:

- How is data securely destroyed when no longer needed?
- Is there a policy or procedure for handling obsolete or unused data?

Section 6: Data Subjects and Privacy Rights

6.1 Categories of Data Subjects:

- Who are the individuals whose data is collected and processed (e.g., customers, merchants)?

6.2 Privacy Rights:

- Are individuals informed of their rights (e.g., to access, correct, or delete their data)?
- How are individuals able to exercise these rights?

6.3 Complaint Resolution Process:

- How can users raise concerns or complaints about their data?
- What procedures are in place to investigate and address these concerns?

Section 7: Accountability and Oversight

7.1 Accountability Measures:

- Who is responsible for overseeing data protection compliance (e.g., Data Protection Officer)?
- Define responsibilities for each phase of the PIA, from implementation to monitoring.

7.2 Monitoring and Updates:

- How frequently is the PIA reviewed?
- What triggers a review (e.g., introduction of new features, regulatory changes)?

Section 8: Post-Implementation Evaluation Metrics

8.1 Compliance Assessment:

- Are the identified risks adequately mitigated, and is compliance maintained with relevant standards?

8.2 Transparency:

- Are users provided with clear and ongoing information about data usage and rights?

8.3 Continuous Improvement:

- Are periodic audits conducted to identify improvements or address new risks.