



University of
Zurich^{UZH}

Privacy Analysis and Compliance Approach with a Focus on Children

Yuanyuan Huang
Zurich, Switzerland
Student ID: 20741310

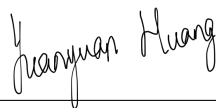
Supervisor: Prof. Dr. Burkhard Stiller, Katharina O. E. Mueller,
Weijie Niu

Date of Submission: August 5th, 2024

Declaration of Independence

I hereby declare that I have composed this work independently and without the use of any aids other than those declared (including generative AI such as ChatGPT). I am aware that I take full responsibility for the scientific character of the submitted text myself, even if AI aids were used and declared (after written confirmation by the supervising professor). All passages taken verbatim or in sense from published or unpublished writings are identified as such. The work has not yet been submitted in the same or similar form or in excerpts as part of another examination.

Zürich,



Signature of student

Abstract

In den letzten Jahren sind mit dem Einsatz tragbarer Technologien eine erhebliche Anzahl von Risiken aufgrund der Erfassung und Verarbeitung sensibler persönlicher Informationen entstanden, insbesondere im Zusammenhang mit den Datenschutz- und Compliance-Herausforderungen im Zusammenhang mit tragbaren Technologien wie Smartwatches für Kinder. In Anbetracht dessen wird in dieser Arbeit eine automatisierte Anwendung zur Überprüfung der Einhaltung umfassender Datenschutzvorschriften, einschliesslich the General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), the New Federal Act on Data Protection (nFADP), Personal Information Protection Law of the People's Republic of China (PIPL) and Protection of Personal Information Act (POPIA), vorgeschlagen. Das System nutzt Techniken Natural Language Processing (NLP), insbesondere das Bidirectional Encoder Representations from Transformers (BERT) Modell, um eine konsistente Bewertung der Einhaltung von Datenschutzstandards durch Smartwatches zu erleichtern. Um dies zu erreichen, umfasst diese Masterarbeit die Analyse von Vorschriften, die Datenbankgestaltung, die Entwicklung von APIs und die Implementierung der Benutzeroberfläche. Die vorgeschlagene Anwendung zielt darauf ab, Erziehungsberechtigten Werkzeuge an die Hand zu geben, um die digitale Privatsphäre von Kindern zu schützen und Gerätehersteller zu motivieren, konformere Geräte zu entwerfen.

In recent years, with wearable technologies being brought to use, a significant number of risks have arisen due to the collection and processing of sensitive personal information, particularly in the context of privacy and compliance challenges associated with wearable technologies such as smartwatches designed for children. Considering this, this thesis proposes an automated compliance checking application aimed at ensuring adherence to comprehensive privacy regulations, including the General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), the New Federal Act on Data Protection (nFADP), Personal Information Protection Law of the People's Republic of China (PIPL) and Protection of Personal Information Act (POPIA). The application leverages Natural Language Processing (NLP) techniques, specifically the Bidirectional Encoder Representations from Transformers (BERT) model, to facilitate consistent evaluation of smartwatches' compliance with privacy standards. To achieve this, the thesis encompasses regulatory analysis, database design, API development, and user interface implementation. The proposed application aims to empower guardians with tools to safeguard children's digital privacy and urge device manufacturers to design more compliant devices.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisors - Prof. Dr. Burkhard Stiller, Katharina O. E. M  ller, and Weijie Niu - for their invaluable guidance, insightful advice, and unwavering support throughout my thesis. Especially, I would like to thank Katharina for her significant contributions and support, she was very responsible and patient during the whole thesis, and I really appreciated it. Her assistance has been very important in shaping the direction and quality of my work. Her expertise and encouragement have been instrumental in the successful completion of this thesis. Additionally, I am profoundly grateful to Weijie for his extensive help with the NLP aspects of this thesis. His willingness to find time for us, even during his vacation, is something for which I am truly thankful.

I would like to extend my heartfelt thanks to my family and friends, especially my mother, who has always been so supportive and encouraging throughout this journey.

To all those who have supported me in any way during my thesis, I offer my sincerest thanks.

Contents

| | |
|---|------------|
| Declaration of Independence | i |
| Abstract | iii |
| Acknowledgments | v |
| 1 Introduction | 1 |
| 1.1 Motivation | 1 |
| 1.2 Thesis Goals | 1 |
| 1.3 Thesis Outline | 2 |
| 2 Fundamentals | 3 |
| 2.1 Background | 3 |
| 2.1.1 Tracking Technology | 3 |
| 2.1.2 Data privacy and security | 6 |
| 2.1.3 Related Regulations | 7 |
| 2.2 Related Work | 11 |
| 3 Design | 13 |
| 3.1 Database Design | 13 |
| 3.1.1 Regulatory Analysis and Synthesis | 13 |
| 3.1.2 Categorization | 15 |
| 3.1.3 Schema Design | 15 |
| 3.1.4 Data Export | 16 |

| | | |
|----------|--|-----------|
| 3.2 | API Development | 16 |
| 3.2.1 | Flask API Development | 16 |
| 3.2.2 | Setting Up Flask: | 17 |
| 3.3 | Automated Compliance Checking | 17 |
| 3.3.1 | Utilizing NLP for Compliance Checking | 18 |
| 3.3.2 | Selection of the BERT Model | 18 |
| 3.3.3 | Approach to Using BERT for Compliance Checking | 18 |
| 3.4 | Comparison between chosen watches | 21 |
| 3.5 | User Interface design | 22 |
| 3.5.1 | Sign-In and Smartwatch Connectivity | 23 |
| 3.5.2 | Area Selection | 24 |
| 3.5.3 | Dashboard Overview and Compliance Scoring | 24 |
| 3.5.4 | Detailed Reporting | 24 |
| 3.5.5 | User Feedback | 24 |
| 3.5.6 | Device Management | 25 |
| 3.5.7 | Navigational Elements | 25 |
| 4 | Implementation | 27 |
| 4.1 | Database Implementation | 27 |
| 4.2 | NLP Implementation | 27 |
| 4.2.1 | Data Splitting | 27 |
| 4.2.2 | Data Augmentation | 28 |
| 4.2.3 | Model Fine-Tuning | 28 |
| 4.2.4 | Model Evaluation | 29 |
| 4.3 | API Implementation | 29 |
| 4.3.1 | API Endpoints and Functionality | 29 |
| 4.4 | User Interface Implementation | 30 |
| 4.4.1 | Sign-In and Smartwatch Connectivity | 30 |

| | |
|--|-----------|
| <i>CONTENTS</i> | ix |
| 4.4.2 Dashboard Overview and Compliance Result | 33 |
| 4.4.3 Detailed Reporting | 34 |
| 4.4.4 User Feedback | 35 |
| 4.4.5 Multiple Device Management | 36 |
| 4.4.6 Navigational Elements | 37 |
| 5 Evaluation | 39 |
| 5.1 NLP Model Evaluation | 39 |
| 5.2 Regulatory Guidelines Evaluation | 41 |
| 5.3 Evaluation on Specific Smartwatch Models: Xplora and Garrett . . . | 42 |
| 5.3.1 Garrett Smartwatch | 43 |
| 5.3.2 Xplora Smartwatch | 44 |
| 5.4 Comparative Analysis with Similar Approaches | 46 |
| 5.4.1 Traditional Manual Auditing | 46 |
| 5.4.2 Other NLP-Based Systems: | 46 |
| 5.5 Summary of Evaluation | 46 |
| 6 Final Considerations | 49 |
| 6.1 Summary | 49 |
| 6.2 Conclusions | 49 |
| 6.3 Future Work | 50 |
| Abbreviations | 61 |
| List of Figures | 61 |
| List of Tables | 63 |
| List of Listings | 66 |

Chapter 1

Introduction

In an era where digital devices are becoming universal in children's lives, smartwatches, while offering potential benefits in terms of connectivity and health monitoring [1], also show significant risks by collecting and processing sensitive personal data [2]. The regulatory landscape such as GDPR and CCPA, while evolving, struggles to keep pace with these technological innovations, leaving gaps in protecting children's sensitive information. This thesis specifically focuses on children's smartwatches and the associated privacy concerns.

1.1 Motivation

The motivation for this thesis originates from the expanding development of wearable technology, particularly smartwatches designed for children.

The focus is set on smartwatches for children for a variety of reasons. Firstly, these devices collect a wide range of data, from locational to health-related information, which, if mishandled, can lead to privacy breaches with long-lasting consequences. Secondly, parents and guardians often lack the technical expertise or resources to comprehensively assess these devices' privacy practices. This thesis is motivated to empower guardians with the knowledge and tools to make informed decisions regarding the digital safety of their children, thereby creating a safer digital environment for the younger generation.

1.2 Thesis Goals

The goal of this thesis is to develop an application that automates the compliance checking process against a comprehensive checklist derived from various privacy policies and regulations, including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), New Federal Act on Data

Protection (nFADP), Personal Information Protection Law of the People’s Republic of China (PIPL), and Protection of Personal Information Act (POPIA) [3, 4, 5, 6, 7].

This application addresses the need for a systematic, user-friendly approach to evaluating children’s smartwatches, bridging the gap between technological advancements in children’s wearables and the legal frameworks established to protect their privacy. By automating the compliance evaluation process, the application helps guardians more directly verify the privacy standards of smartwatches used by children. The initiative aims to streamline the process of identifying non-compliance issues, provide guardians with an easy-to-use tool, and help device manufacturers design products with greater attention to privacy and security.

Through this work, this thesis aspires to enhance the digital safety of children through privacy compliance checks and to help develop more strict privacy standards in children’s digital devices.

1.3 Thesis Outline

This thesis is structured to provide a comprehensive analysis and solution for ensuring the privacy and security compliance of smartwatches designed for children.

Chapter 1 introduces the motivation behind the thesis, the specific goals aimed to be achieved, and a brief outline of the thesis structure. Chapter 2 shows the fundamental concepts that are necessary for understanding the research context, including tracking technology, data privacy and security, and related privacy policies, as well as a review of related work in the field. Chapter 3 details the design phase of the application, including the database design, regulatory analysis and synthesis, API design using Flask, the analysis of Natural Language Processing (NLP) for automated compliance checking, particularly focusing on the BERT model and the integration of these components into a compliance checking application. Chapter 4 discusses the implementation of the proposed application, starting with the database schema, followed by the setup of the Flask API, the NLP implementation, the integration with Android Studio, and the user interface implementation. Chapter 5 provides a thorough evaluation of the application, including an assessment of the NLP model’s performance, an evaluation against regulatory guidelines, a comparative analysis with similar approaches, and a specific evaluation of the chosen smartwatches. Finally, Chapter 6 concludes the thesis with a summary of findings, conclusions drawn from the research, and potential directions for future work.

Chapter 2

Fundamentals

This chapter explores the increasing popularity of tracking technologies in children’s smartwatches. However, it also addresses significant privacy and security concerns brought by it, emphasizing the need for robust data protection and adherence to international regulations like the CCPA, GDPR, nFADP, POPIA, and PIPL.

2.1 Background

In recent years, devices embedded with tracking technology, such as smartwatches, have become more and more popular [8]. Meanwhile, it has also raised people’s concerns about personal and public safety [9]. These devices are increasingly marketed to guardians as essential tools for ensuring peace of mind and monitoring their children’s whereabouts. Consequently, new regulations such as PIPL which are newly proposed and effected in November 2021[5] are being introduced to address the growing need for robust privacy and security standards in these innovative products.

2.1.1 Tracking Technology

Among all common tracking technologies, Global Positioning System (GPS)-enabled devices, Wi-Fi, cellular, and Bluetooth technologies have been at the forefront, offering real-time location tracking [10].

GPS technology

The beginning of tracking technologies can be traced back to military applications, with GPS initially developed and utilized by the United States Department of Defense [11]. GPS works by transmitting signals from satellites in space to

GPS receivers on the ground, allowing the receivers to calculate their exact location (latitude, longitude, and altitude) with remarkable accuracy [12]. However, its transition to civilian use in the late 20th century marked the beginning of its widespread adoption for navigation, asset tracking, and personal safety [13]. The integration of these technologies into consumer devices has been facilitated by advancements in miniaturization, battery life, and wireless communication, enabling the development of portable, user-friendly devices tailored for children [14]. From a technical perspective, the utilization of GPS data requires robust encryption methods to protect the data in transit and at rest. For instance, data transmitted from the smartwatch to cloud servers or between the watch and a paired smartphone should employ secure communication protocols like HTTPS, incorporating TLS (Transport Layer Security) encryption to safeguard against interception or tampering [15]. Integrating GPS technology into smartwatches introduces several technical challenges and considerations, particularly concerning data privacy and security as described in section 2.1.2. For example, devices require encryption to prevent unauthorized access, especially if the device is lost or compromised. Additionally, the precise nature of GPS data raises significant privacy concerns, as it can reveal detailed information about an individual's movements and habits [16]. Therefore, implementing comprehensive data minimization practices is crucial, ensuring that only the necessary location data is collected for the intended functionality, and retaining it only as long as needed [17].

Wi-Fi technology

While GPS excels in outdoor environments, its accuracy can decrease in urban settings or indoors due to signal blockage from buildings and other structures. This is where Wi-Fi positioning can be helpful. Wi-Fi-based location tracking uses the signals from local Wi-Fi networks to determine a device's location [18]. In most modern urban areas, the density of Wi-Fi networks allows for the signal strength of multiple nearby Wi-Fi access points to be used for triangulating the position of a device, typically by measuring the Received Signal Strength Indicator (RSSI) of each access point [19, 20]. This method enhances location accuracy in places where GPS might falter, providing a complementary solution for indoor and urban area tracking [21]. The integration of Wi-Fi technology in smartwatches extends their connectivity and functionality, enabling direct access to the internet and cloud-based services without relying on a paired smartphone. However, this connectivity introduces technical challenges related to security and privacy. Wi-Fi connections which are less secure than wired connections, are susceptible to various attacks such as eavesdropping, man-in-the-middle attacks, and unauthorized access [22]. To mitigate these risks, smartwatches implement robust security protocols like WPA3, which offers enhanced encryption and improved security features compared to its predecessor, WPA2 [23]. One of the key advancements is the use of Simultaneous Authentication of Equals (SAE), which provides better protection against offline dictionary attacks. This means that even if a password is weak, WPA3 significantly reduces the likelihood of it being cracked through brute force attempts [24]. From a privacy standpoint, Wi-Fi connectivity can potentially

expose user location through network identification and tracking. To address this, smartwatches often employ measures such as randomized MAC addresses and VPN usage to anonymize connections and protect users' location privacy [25].

Cellular technology

Similar to Wifi's distance calculation method as described in section 2.1.1, cellular tracking technology leverages the widespread and dense network of cell phone towers to determine a device's location [26]. This form of tracking calculates a device's position based on its distance from multiple cell towers. It uses techniques like multilateration [27] to measure the time signals take to travel between the device and the towers. By triangulating these distances, the system can accurately estimate the device's location, which is particularly useful in urban areas with high cell tower density [28]. While cellular tracking may not be as accurate as GPS, it does provide valuable location information where GPS and Wi-Fi might not be available, ensuring continuous coverage. The adoption of cellular technology in smartwatches significantly enhances their utility, enabling them to function independently of a smartphone for communication and data access. However, this standalone connectivity introduces complex security and privacy challenges. Cellular networks, while generally secure, can still be vulnerable to threats such as interception, SIM swapping attacks, and location tracking vulnerabilities [29]. To combat these risks, smartwatches leverage advanced encryption protocols within cellular standards, such as the use of AES encryption in 4G LTE and the enhanced security features of 5G, which include stronger user privacy protections against tracking and eavesdropping [30, 31]. Moreover, to safeguard user privacy, smartwatch manufacturers must implement rigorous data protection measures, ensuring that sensitive information, such as call logs and messages, is securely encrypted on the device.

Bluetooth technology

Bluetooth relies on short-range radio frequency, and any device that incorporates the technology can communicate as long as it is within the required distance [32]. The technology is often used to allow two different types of devices to communicate with each other [33]. The integration of Bluetooth technology in smartwatches facilitates seamless communication with smartphones and other Bluetooth-enabled devices, enhancing user convenience through wireless connectivity. However, this convenience brings security challenges such as unauthorized access, and privacy challenges such as data leakage and device tracking [34]. For example, if the Bluetooth address is not properly randomized, it can be used to track the child's movements and activities over time [35]. To mitigate these risks, Bluetooth technology incorporates several security features such as frequency hopping -spreading the Bluetooth signal over rapidly changing frequencies, reducing the likelihood

of interference [36]. Furthermore, Bluetooth Low Energy (BLE) introduces additional privacy measures like address randomization, which changes the device's Bluetooth address frequently to prevent long-term tracking [37].

Table 2.1 compares these four technologies in terms of tracking method, triangulation technique, distance calculation accuracy, advantages, and limitations. Each of them has strengths and weaknesses in terms of tracking technology, making them suitable for different scenarios. However, these benefits are accompanied by distinct security and privacy challenges.

Table 2.1: Comparison of GPS, Cellular, Bluetooth, and Wi-Fi tracking technologies

| Aspect | GPS | Cellular | Bluetooth | Wi-Fi |
|------------------------------|--------------------------------------|--|---|--|
| Tracking | Using satellites | Proximity to cell towers | Short-range radio waves | Signal strength from access points |
| Triangulation | Trilateration from satellite signals | Multilateration using cell tower signals | Signal strength from multiple BLE beacons | Signal strength from multiple Wi-Fi points |
| Distance Calculations | Very precise, within 5-10 meters | Varies, 100 meters to a few kilometers | Accurate within 10 meters | Accurate within 20-30 meters |
| Advantages | High accuracy, global coverage | Works indoors, effective in urban areas | Low power, effective indoors | Works indoors, widely available |
| Limitations | Less effective indoors | Less accurate (dependent on tower density) | Limited range, affected by obstacles | Less accurate (dependent on Wi-Fi network density) |

2.1.2 Data privacy and security

Data privacy, also called "information privacy", is the principle that a person should have control over their personal data, including the ability to decide how organizations collect, store and use their data [38]. Data privacy is a crucial aspect of children's smartwatches as these devices collect and store sensitive information, such as location, activity logs, and personal data .

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle [39]. This concept covers the full range of information security, including the physical security of hardware

and storage devices, as well as administrative and access controls. It also includes the logical security of software applications as well as organizational policies and procedures [39]. Ensuring data security in child safety devices is crucial because it directly impacts the privacy of the children using them. If a data leak occurs, this information could be very dangerous in the wrong hands.

The market for children’s smartwatches has grown rapidly, driven by parental demand for solutions that can help keep their children safe [40]. These devices often come equipped with a variety of features, including two-way communication, SOS buttons, and geofencing capabilities, allowing parents to set boundaries and receive alerts if their child enters or leaves a designated area [41]. Since the introduction of the AirTag in 2021, consumers have become more aware of the possible pitfalls of IoT devices, especially in use cases such as personal tracking devices [34]. With a lawsuit being started by two women who found an AirTag on her car, and the other finding it in her child’s backpack [42], concerns have been raised about data privacy and data security - unauthorized tracking, unauthorized access, data breaches and leaks, compliance with privacy regulations, and the psychological impact of surveillance on children’s development [43].

Unauthorized tracking and unauthorized access are significant concerns regarding children’s smartwatches. Unauthorized tracking refers to the ability of malicious actors to monitor a child’s location without consent, often due to inadequate security measures like weak encryption or default passwords [44]. This can lead to severe privacy violations, exposing children to potential physical dangers. Unauthorized access involves hackers exploiting security flaws to intercept communications or take control of the device, allowing them to listen to conversations, view messages, or even manipulate the smartwatch’s functions [45].

Data breaches and leaks in children’s smartwatches occur when sensitive information is accessed or disclosed without authorization. These incidents can severely affect children’s data privacy and security by exposing them to identity theft, stalking, or other malicious activities. Misuse of personal information involves exploiting this data for purposes other than intended, such as marketing, tracking, or even blackmail [46].

Compliance with privacy regulations involves adhering to laws and guidelines designed to protect the personal data of individuals, particularly minors. For children’s smartwatches, this means ensuring that data collection, processing, and storage practices meet the standards set by laws. Non-compliance can lead to significant privacy breaches, putting children’s sensitive information at risk of unauthorized access, misuse, and exploitation [47].

2.1.3 Related Regulations

Moreover, the privacy policies concerning the protection of children’s data embody the principle that minors require special safeguards and privacy considerations, especially in the rapidly evolving digital realm. However, the regulatory landscape

for children’s smartwatches remains fragmented, with varying standards and guidelines across different jurisdictions. The CCPA, GDPR, PIPL, nFADP, and POPIA outline distinct strategies and legal frameworks to uphold children’s digital privacy rights.

The GDPR [6] is a comprehensive data protection law in the European Union that establishes privacy rights for individuals and obligations for organizations regarding the collection, processing, and free movement of personal data. The GDPR sets forth that children under 16 (or a lower age if permitted by a member state, not below 13) require parental consent for data processing in the context of information society services, which include online services and digital platforms like social media, e-commerce, and cloud services. It highlights the need for clear and affirmative consent for all data processing activities and mandates special attention for activities directed at children. GDPR has a broad extraterritorial scope, applying to any organization worldwide that processes the data of individuals within the EU. The GDPR is often seen as the most stringent and comprehensive, influencing global data protection standards.

The CCPA [3] enhances consumer privacy rights by granting California residents specific rights, including the right to know, delete, and opt-out of the sale of personal information, with special protections for children under 16. It requires businesses to obtain affirmative consent from consumers under 16 and obtain verifiable parental consent for those under 13 before collecting or selling personal information. The law also establishes a Consumer Privacy Fund, which, among other purposes, is used to educate children about online privacy. CCPA applies to businesses operating in California, impacting global companies by requiring them to comply with its data privacy standards when handling the personal information of California residents. Compared to GDPR, the CCPA is less stringent and comprehensive but marks a significant step in U.S. data protection, particularly with its focus on consumer rights and business obligations.

The PIPL [5] is China’s data protection legislation that regulates the processing of personal data and enhances the privacy rights of individuals within China. PIPL in China designates the personal information of minors under 14 as sensitive, mandating that consent from parents or guardians is obtained before processing such data. It calls for processors to formulate specific rules for handling the personal information of minors. PIPL similarly applies to organizations operating within China or those outside of China processing the personal information of Chinese residents to provide products or services or analyze and evaluate the behavior of residents within China.

The nFADP [7] is Switzerland’s data protection law that governs the processing of personal data by private entities and federal bodies, emphasizing transparency, proportionality, and data security. The nFADP of Switzerland does not differentiate between the data of children and adults, treating all personal data under the same general privacy protections without special provisions for minors. nFADP applies to all individuals and businesses processing data in Switzerland or from Swiss

residents, regardless of the age of the data subject, promoting a one-size-fits-all approach within its jurisdiction.

The POPIA [4] is South Africa’s comprehensive data protection law that regulates the processing of personal information and upholds the right to privacy. POPIA from South Africa permits the processing of children’s ¹ personal data with the consent of a competent person, such as a parent or guardian. It places conditions on this processing and emphasizes protecting the interests of the child, particularly in cases where the child’s data is processed for public or legal interests. POPIA affects any entity that processes personal data within the South African border, as well as those outside South Africa that process data in a manner that infringes on the privacy rights of South African residents.

Global privacy policies aimed at handling children’s data show a strong effort to protect young people in our increasingly digital world. The CCPA, GDPR, PIPL, and POPIA all emphasize children’s privacy, while the nFADP takes children as the same as adults in terms of privacy and data security. Despite the complexities these varied regulations introduce, they share a common goal: enhancing the defenses around the digital activities of minors and ensuring robust data security and privacy measures, as shown in Table 2.2. The broader concern encompasses preventing inappropriate use of minors’ data for profiling or targeted advertising and guarding against undue privacy intrusions. These regulations develop to become more comprehensible to protect children’s privacy [48] by requiring companies to uphold stringent data protection protocols.

¹”child” means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself.

Table 2.2: Comparison of Children’s Privacy Regulations: CCPA, GDPR, POPIA, PIPL, nFADP

| Aspect | CCPA (California) | GDPR (EU) | POPIA (South Africa) | PIPL (China) | nFADP (Switzerland) |
|---|--|---|--|---|---|
| User Consent and Data Usage | Requires explicit consent for data sale; opt-in options for minors | Requires explicit consent for data processing; opt-in for children under 16 | Requires explicit consent; opt-in for minors under 18 | Requires explicit consent for data processing; opt-in for children under 14 | Requires explicit consent for data processing; opt-in for children under 16 |
| Data Management and Rights | Rights to access, delete, and opt-out of data sale | Rights to access, rectify, erase, restrict processing, and data portability | Rights to access, rectify, and erase data | Rights to access, rectify, erase, restrict processing, and data portability | Rights to access, rectify, and erase data |
| Privacy Policies and Practices - Data Handling | Specific provisions for data collection, processing, and sharing; enhanced protections for children’s data | Detailed rules for data processing, collection, and sharing | Specific measures for data collection and processing | Strict rules for data collection, processing, and sharing | Specific provisions for data handling |
| Children’s Safety | Enhanced protections and explicit consent requirements for children’s data | Specific rules for processing minors’ data; parental consent required | Specific protection measures and parental consent for minors | Strict protection measures and parental consent for children’s data | Enhanced protections and adherence to best practices for minors |
| Advertising and Tracking | Opt-out mechanisms for behavioral advertising; restrictions on data use for advertising | Restrictions on profiling and behavioral advertising; explicit consent required | Restrictions on data use for advertising; consent required | Restrictions on data use for advertising; clear consent requirements | Restrictions on data use for advertising |

Since the fast-paced development of tracking devices and their increasing presence in the lives of children, especially through wearable devices like smartwatches, offering both unprecedented safety features and potential risks, the need for a comprehensive analysis of their impact on privacy becomes essential. This thesis will undertake an exploration of the current state of child monitoring technologies, focusing on smartwatches. It will examine how current smartwatches comply with stringent privacy regulations in various jurisdictions and assess their effectiveness in keeping children safe without compromising their rights as described in Chapter 3. The goal of this thesis is to raise parents' awareness and urge companies to design smartwatches for children that are especially compliant with related regulations.

2.2 Related Work

This section reviews relevant studies and developments concerning tracking technologies, with a special focus on their application in children's smartwatches, privacy and security concerns, and regulatory compliance issues.

Tracking technologies such as the Wi-Fi Positioning System (WPS), Cellular Network Tracking, Global Positioning System (GPS), and Bluetooth Low Energy (BLE) Beacons constitute the core of modern tracking solutions. Despite their widespread application, Wi-Fi and BLE face reliability issues in information transmission due to inconsistent coverage [49, 50]. Cellular connectivity's limitations similarly affect tracking accuracy [51]. GPS is increasingly being used to track human beings, and one of the applications is to use the technology to track children [52]. Much of the legal concern surrounding GPS tracking has focused on privacy concerns - who has access to the data generated by GPS tracking is clearly a legitimate concern, it is the fact that such data are generated that are often not examined closely [53].

The Norwegian Consumer Council's research conducted in 2017 first highlighted the vulnerabilities associated with the lack of data protection in connected toys and their supporting infrastructure [54], leading some agencies, such as the German Federal Telecommunications Agency (Bundesnetzagentur), to prohibit the sale of smartwatches for children [55]. In 2019, Avast researchers independently identified vulnerabilities in 29 GPS tracker models produced by Shenzhen i365 Tech, a white-label manufacturer utilizing the AIBEILE backend. These vulnerabilities encompass the potential for unauthorized tracking, wiretapping, and location spoofing of the devices [56]. [57] in 2023 revealed significant security vulnerabilities in several popular kids' smartwatches when exploited by SMS command injection, Bluetooth tracking and Wi-Fi man in the middle attack. Additionally, multiple vendors explicitly state that their watches do not have a remote monitor functionality, because it would be illegal under various jurisdictions. This marketing promise is, however, severely contradicted by third-party apps available in app stores - the FindMyKids application [58] for example, advertising this functionality on the same platform [59].

The regulatory landscape for children’s smartwatches is complex and fragmented. Organizations are under pressure to be compliant with a range of privacy legislation, policies, and best practices. At the same time, many firms are using privacy as a key differentiator [60]. [55] mentioned in their paper the considered low-end devices are broadly speaking less secure than high-end ones, most of them present security and privacy flaws, which illustrates the necessity of regulation that ensures the fulfillment of appropriate security and privacy requirements. [61] in 2018 introduced an automated framework to evaluate the privacy compliance of 5,855 children’s apps with COPPA, revealing widespread potential violations primarily due to third-party software development kits (SDKs). Notably, 19% of these apps improperly collect personally identifiable information (PII), despite explicit prohibitions in SDK terms for child-directed applications. This body of work underscores the critical need for stringent regulatory frameworks to protect children in the digital age. [62] suggest that most developers rely on app markets to identify privacy issues, they lack a complete understanding of the third-party SDKs they integrate, and they find it challenging to ensure that these SDKs are kept up-to-date and privacy-related options are configured correctly. [63] developed a novel method to accurately retrieve the expectations, privacy risk mitigation areas, and the associated regulations using Natural Language Processing and Semantic Web concepts.

The literature on children’s smartwatches and tracking technologies reveals a landscape filled with technological promise and complex ethical considerations. While these devices offer substantial benefits in terms of child safety, they also pose significant privacy, security, and developmental challenges. This thesis builds upon the existing literature by not only highlighting these issues but also by proposing practical solution to enhance the compliance and ethical deployment of child monitoring technologies.

Chapter 3

Design

This thesis aims to design a system for evaluating the compliance of smartwatches with established child-related privacy policies and regulations. The cornerstone is the development of a robust, scalable application that includes a local relational database in Android Studio, a RESTful API for seamless data interaction, and an automated compliance checking mechanism utilizing NLP. The results are then sent back to a user interface designed in Android Studio, ensuring a user-friendly experience for guardians. This section details the architectural design and the reasons behind the choice of technologies and methodologies employed, ensuring the system effectively identifies compliance issues.

3.1 Database Design

The database design segment involves storing related policies and regulations in a local database in Android Studio. Local databases offer efficient data management and quick retrieval. Additionally, since the dataset is not large, a local database is sufficient for storing and managing the information. It also simplifies data synchronization and reduces dependency on external servers, lowering costs and improving data security by limiting exposure to network vulnerabilities, and can help maintain reliable and responsive service even when the mobile device does not have a reliable connection [64]. This structured approach to data storage is crucial for subsequent regulatory analysis, as it allows for easy access and organization of the information.

3.1.1 Regulatory Analysis and Synthesis

For the regulations, the cornerstone is to create a compliance checklist, which represents a schematic against which each smartwatch can be compared to assess their compliance and evaluate the extent of the compliance. This process began with a legal research phase focusing on privacy laws and guidelines relevant to children's

digital devices, including GDPR, CCPA, PIPL, nFADP, and POPIA. The goal of this legal research was to identify specific provisions and obligations applied to smartwatch manufacturers, particularly those concerning data collection, storage, consent mechanisms, and user rights, as shown in section 2.1.3.

First, the regulation texts were read to understand their key provisions and requirements. The major sections of the regulations were identified, which involved highlighting specific clauses that mandate what information must be provided to consumers and the rights afforded to them. From these key provisions, relevant clauses that dictate the necessary components of a privacy policy and consumer notifications were extracted. For instance, the CCPA requires businesses to disclose: The categories of personal data collected; The purposes for data collection; The third parties with whom data is shared; The consumer rights regarding their personal data, including access, deletion, and opt-out rights [3]. Using these extracted clauses, initial questions were formulated that a business must address to ensure compliance with the regulations. Each question corresponds to a specific requirement in the regulation.

To enhance the comprehensiveness of the checklists, online research was conducted, including reviewing guidelines from official regulatory bodies and industry best practices [65, 66, 67, 68, 69]. This process involved examining multiple regulatory frameworks and standards, comparing their requirements, and identifying both commonalities and unique aspects. The aim was to cross-reference these sources to ensure that the checklists cover all relevant aspects such as data collection, processing, storage, user consent, and data security measures from each regulation.

As shown in Table 3.1, the checklist example includes various questions to ensure compliance.

Table 3.1: Example of checklist

| checklist | question |
|-----------|--|
| ccpa | Have you created a comprehensive Privacy Policy informing consumers at or before the point of data collection about how data is collected, retained, and used? |
| ccpa | Does your Privacy Policy inform consumers about the categories of personal data collected and the purposes for which it is collected? |
| ccpa | Does your Privacy Policy disclose whether collected data is sold to or shared with third parties and identify those third parties? |
| ccpa | Does your Privacy Policy inform website visitors of their privacy rights and how to exercise them? |
| ccpa | Is your Privacy Policy clear, easy to understand, and available in the languages in which your business provides information in California? |

3.1.2 Categorization

With this preliminary list of compliance criteria, the next step involved categorizing these criteria based on their impact on child privacy and safety. To ensure comprehensive coverage of privacy and security aspects applied to smartwatches for children, the compliance checking framework was structured into several key categories that are fundamental elements of most data protection regulations and are critical for compliance and protecting user privacy:

- **User Consent and Data Usage:** Examines mechanisms for obtaining and managing user consent and how data is utilized, it ensures that users are informed about and agree to the collection and use of their data, and impacts security by ensuring users are aware of and consent to data collection.
- **Data Management and Rights:** Focuses on storage, security, and user rights like data access, correction, and deletion concerning their data.
- **Privacy Policies and Practices - Data Handling:** Details the specifics of data collection, processing, and sharing, ensuring that users understand and agree to these practices.
- **Children's Safety:** Includes special considerations for collecting and using children's data.
- **Advertising and Tracking:** Addresses the use of data for advertising purposes and the presence of tracking mechanisms, ensuring that data used for advertising is protected against unauthorized access and breaches.

Each of these categories is crucial for evaluating the adherence of smartwatches to established child-related privacy policies and regulations. It ensures a structured and comprehensive evaluation of smartwatch adherence to child-related privacy regulations. The complete final checklist can be found in the appendix 3.

3.1.3 Schema Design

The SQLite database schema was designed to store and manage the checklist items efficiently. SQLite was chosen for its robustness and efficiency in managing lightweight data storage and retrieval tasks, and the database was integrated into an Android Studio project, leveraging SQLite's capabilities to handle the data requirements of the application.

The primary tables included:

Privacy Policies Table: Contains the ID, the name of each watch, and policy details about each watch's privacy policy document.

Checklists Table: Stores the individual checklist items, with the ID, the name

of the checklist, and a description of questions. Each question will be manually answered with a yes/no or not mentioned format (Replaced with 1 for yes, 0 for no or not mentioned).



Figure 3.1: Checklist Schema

The checklist items were systematically organized and stored within the SQLite database. This involved data entry, ensuring accurate categorization and completeness, and establishing relationships between the tables.

3.1.4 Data Export

After that, the dataset which stored 169 checklist questions and 2 watches' policies was exported and transferred to a Python-based environment for advanced NLP analysis.

3.2 API Development

Following the database design, the next critical component was the design of an API to facilitate communication between the Android application and the Python server for NLP analysis. This section details the API design using Flask, a lightweight web framework for Python, and the integration of VS Code with Android Studio for seamless development.

3.2.1 Flask API Development

The primary objective of the API was to enable efficient data transfer between the SQLite database on the Android device and the Python server for further processing. The API was designed to handle requests for exporting checklist data, initiating NLP analysis, and retrieving analysis results, as shown in Figure 3.2.

3.2.2 Setting Up Flask:

Flask was chosen for its simplicity and flexibility in creating RESTful APIs. The Flask application was configured to run on a Python server, with routes defined for each required operation.

Export Data Route: A route to handle requests for exporting checklist data from the SQLite database to the Python server. This route included functionality to serialize the data into JSON format.

Initiate Analysis Route: A route to trigger the NLP analysis on the exported data. This route invoked the necessary NLP processing functions.

Retrieve Results Route: A route to retrieve the results of the NLP analysis, providing a summary of insights and compliance status.

The API design using Flask facilitated efficient communication between the Android application and the Python server, enabling advanced NLP analysis of the compliance checklists.

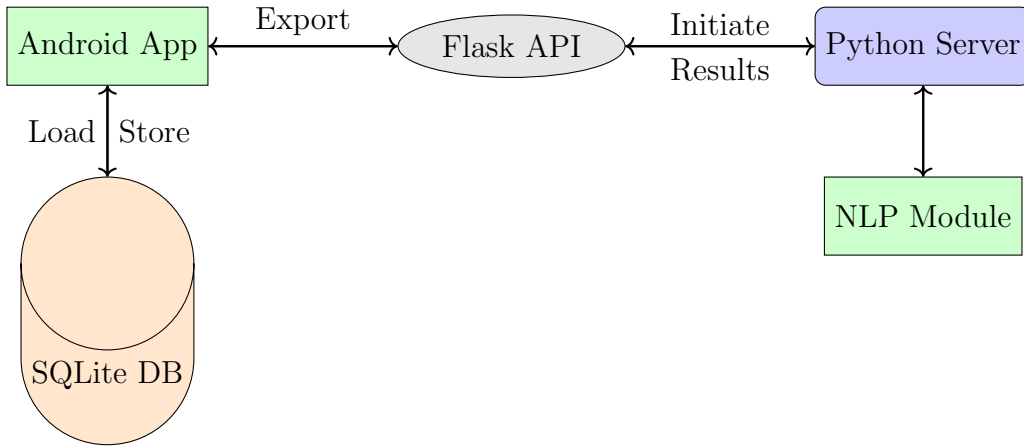


Figure 3.2: API development architecture diagram

3.3 Automated Compliance Checking

The Automated Compliance Checking system is a critical component of this thesis, aimed at ensuring that smartwatches designed for children adhere to strict privacy standards and legal requirements. This section outlines the design rationale behind utilizing NLP for compliance checking, the selection of the BERT model, and the overall approach to leveraging BERT for effective compliance analysis.

3.3.1 Utilizing NLP for Compliance Checking

NLP was chosen as the core technology for the Automated Compliance Checking system due to its capability to analyze and interpret textual data efficiently. Typical compliance management solutions focus on manually identifying the subjects responsible for compliance from paragraphs or statements contained in regulatory documents [70], which can be a very time-consuming, costly, and inefficient process prone to errors, while NLP allows for the automated processing of extensive regulatory documents and privacy policies, and it ensures consistent interpretation of compliance criteria, eliminating human error and subjective bias.

3.3.2 Selection of the BERT Model

Currently, the BERT model released by Google AI Language is considered to be the state-of-the-art language representation model [71]. Recent advances in the NLP literature show that fine-tuning large-scale language models like BERT often yields accurate models for many downstream tasks [72, 73, 74], including Text Classification, Named Entity Recognition, Named Entity Recognition, Text Summarization, and Semantic Search. For this thesis, compliance checking involves analyzing policies and regulations to ensure they meet specified legal or regulatory requirements. In NLP, this task would involve interpreting and understanding textual data to check for compliance criteria which is a downstream task. As a result, the BERT model was selected due to its superior performance in understanding and processing natural language.

3.3.3 Approach to Using BERT for Compliance Checking

Table 3.2 showed an example of the Xplora watch policy from the whole policy, which are extracted from their official website [75, 76], see appendix 1 and 2 for the whole policy. This example highlights the various data points collected by the watch, such as location data, communication logs, and health metrics, and the corresponding privacy practices implemented by the manufacturer.

Table 3.2: Privacy Policy example

| policy_id | watch_name | policy |
|-----------|------------|--|
| 1 | xplora | <p>Article 1. General Provisions</p> <p>The Xplora Watch can, together with the accompanying app and mobile telephone services subscription, collect and transmit data to XPLORA Mobile AS / XPLORA TECHNOLOGIES AS / Xplora Technologies Ltd, such as location data. Such detailed data collection and use is critical to the successful operation of the Xplora Watch. Data collection, storage and use of data will be managed with strict privacy and security measures.</p> <p>Xplora App and Platform collect personal information when a user (hereinafter "you" or "Member") registers with Xplora.</p> <p>"Personal information" is information that identifies or can identify you or the User, such as your name, address, location data, or other data that can be reasonably linked to such information.</p> <p>We very much appreciate the importance of your personal information complying with all regulations and telecommunication acts, including but not limited to national Data Protection regulation as well as EU GDPR.</p> <p>We do our best to protect your personal information by implementing reasonable security standards and hereby inform you of the purposes and methods by which we may use your personal information and of the actions taken to protect your privacy.</p> <p>Article 2. Data Controllers and Data Processors. Access, rectification and deletion</p> <p>For Nordic users (Norway, Sweden, Denmark, Finland and Iceland) Xplora Mobile AS, org. no. 814 499 022, is the Data Controller. For users in the other EU countries...</p> |

Table 3.3 showed an example of the checklist questions of CCPA regulation.

Table 3.3: Compliance Checklist Example

| User Consent and Data Usage | | | |
|-----------------------------|-----------|--|--------|
| Policy ID | Checklist | Question | Answer |
| 1 | CCPA | Have you created a comprehensive Privacy Policy informing consumers at or before the point of data collection about how data is collected, retained, and used? | 1 |
| 1 | CCPA | Does your Privacy Policy inform consumers about the categories of personal data collected and the purposes for which it is collected? | 1 |
| 1 | CCPA | Does your Privacy Policy disclose whether collected data is sold to or shared with third parties and identify those third parties? | 1 |
| 1 | CCPA | Have you obtained consent from a parent or guardian before collecting personal data from children? | 1 |
| 1 | CCPA | Do you obtain explicit consent from the data subject before processing sensitive personal data or personal data from minors between the ages of 13 and 16? | 0 |

In the datasets, for dataset policy 3.2, and dataset regulation 3.3, the text data was cleaned, tokenized, and encoded into a suitable format for BERT. These tables show the example of the compliance checklist dataset for the nlp process, the whole dataset can be found in the appendix 1, 2 and 3.

Due to the size of the dataset being relatively small (338 data in total), Data augmentation was applied, to create a more varied dataset. Additionally, regulatory compliance datasets may often be imbalanced, with certain categories or types of questions being underrepresented, data augmentation can help balance the dataset, ensuring the model performs well across all categories. If any categories perform badly, augmentation can be applied again for a better performance .

After that, the Pre-trained Bert model was first loaded as a base, since it has been trained on large and diverse corpora, and possesses a strong understanding of general language patterns and nuances. By fine-tuning these models on our specific privacy and regulation datasets, we adapt their extensive pre-learned linguistic knowledge to the nuances of the particular task at hand, leading to better accuracy and performance. Then transfer learning techniques were applied for compliance checking tasks, and supervised learning was used to adjust model parameters for improved accuracy in classifying compliance criteria.

For the evaluation, a training loss vs. validation loss plot was generated, to show how well the model was trained, and if there is overfitting/underfitting. Additionally, a separate test set was used to evaluate the model's performance during training, ensuring that metrics such as accuracy, precision, recall, and F1-score

were used to assess effectiveness.

In the end, the compliance check result with a 1/0 label will be transferred back to yes/no and compiled into a compliance report.

3.4 Comparison between chosen watches

Table 3.4 provides a comparative analysis of two smartwatches, Xplora and Garrett, across several critical aspects: tracking technology, app features, data storage, and compliance with regulations. Xplora and Garrett were chosen due to their availability of detailed privacy policies, and their technical specifications. Xplora smartwatches are equipped with GPS tracking, camera functionality, Wifi and 4G connectivity, making them suitable for real-time location monitoring and communication. Garrett smartwatches, on the other hand, feature advanced GPS tracking, Wifi and 4G connectivity, geofencing capabilities, and SOS emergency calling, providing enhanced safety and security tracking functions. These diverse features allow for a thorough assessment of the compliance checking application. Additionally, they are popular among parents - Xplora has sold 1.2 million devices worldwide, Garrett sells over various e-commerce platforms and has an average rating of 4.9 stars from users. [77, 78].

Table 3.4: Feature comparison between Xplora and Garrett smartwatches

| Aspect | Xplora | Garrett |
|------------------------------------|--|---|
| Tracking Technology | GPS, Wi-Fi Mobile network triangulation (not possible to turn off GPS tracking updates. It updates automatically every few minutes.) | GPS, Wi-Fi tracking GPS location updates location at all times |
| App Features | Refresh the location in the Xplora App Activate live tracking in the Xplora App Allow the watch to update the location automatically every few minutes | Activity tracking: Health monitoring Notifications SOS button |
| Data Storage | Location history of the watch is stored for 72 hours, in line with GDPR laws. | Not specified (information not available) |
| Compliance with Regulations | Complies with GDPR regulations. Privacy policy updated regularly to reflect changes in regulations. | Complies with relevant regulations, including GDPR. Policies reviewed and updated. |

3.5 User Interface design

We introduce a user-friendly interface (UI) tailored to facilitate intuitive interaction between the user and the smartwatch compliance checking application. The UI is conceptualized to guide users seamlessly from initial interaction to detailed compliance insights, ensuring a user-friendly experience while providing comprehensive feedback on the smartwatch's privacy and security posture, the overall flow as shown in Figure 3.3.

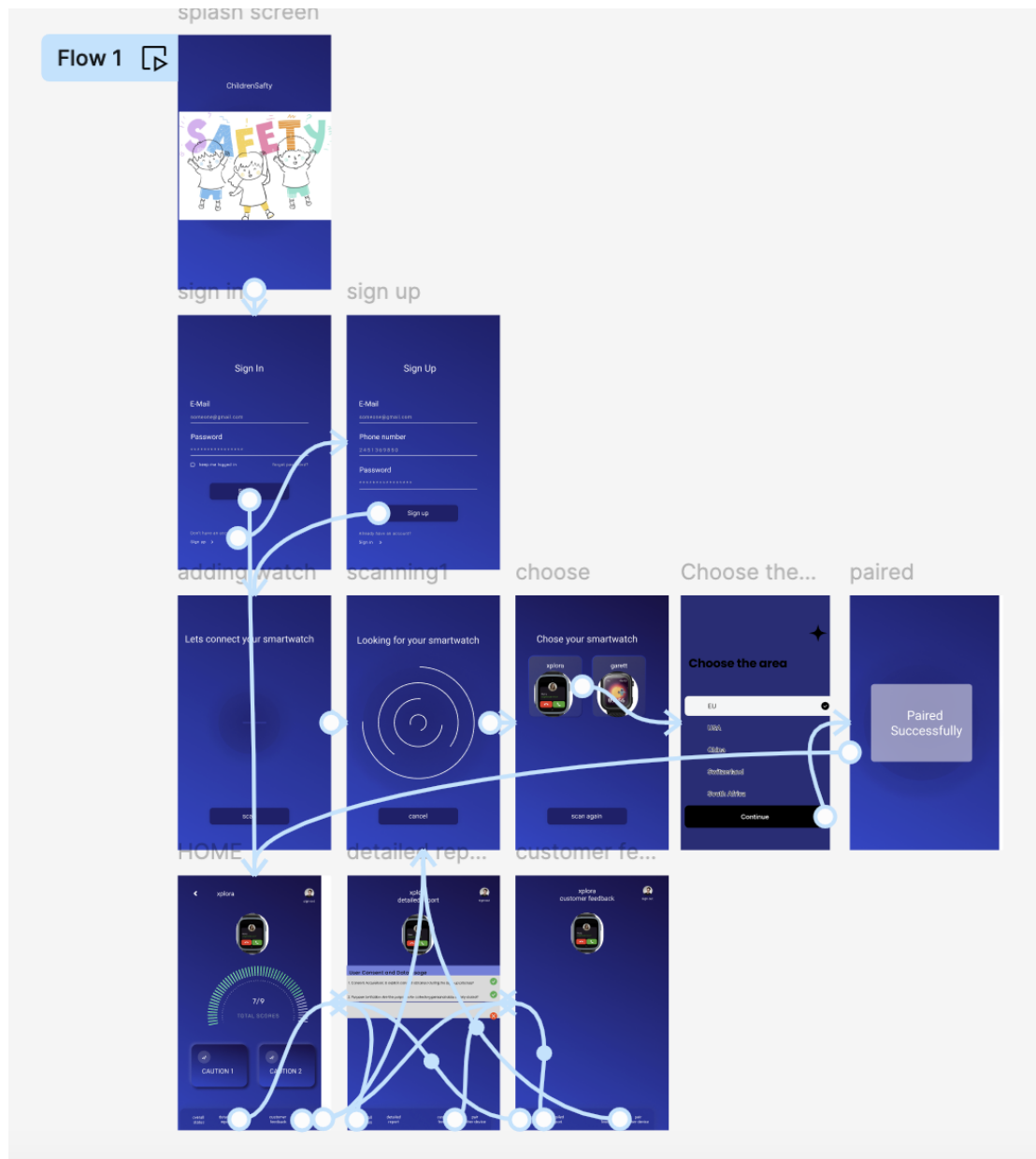


Figure 3.3: UI Design

3.5.1 Sign-In and Smartwatch Connectivity

Upon launching the application, users are greeted with a splash screen first, then a straightforward Sign-In/Sign-Up interface, designed for ease of access while maintaining secure authentication protocols. Following authentication, the application proceeds to connect with nearby smartwatches. This process is accompanied by on-screen instructions and visual cues to assist users in selecting their devices.

Having a Sign-In layout also makes it easier for users to use for the long term, since after the user logs in, they will be directly guided to the dashboard layout,

there is no need to search and add the device again.

3.5.2 Area Selection

A crucial feature of the user interface is the Area Selection screen, where users can choose their geographical region. This selection ensures that the compliance results are tailored to the specific regulations applicable in that area. Users can select from regions such as the EU, USA, China, Switzerland, and South Africa (corresponds to GDPR, CCPA, PIPL, nFADP, and POPIA), ensuring that the compliance analysis is relevant to the regulatory environment in which the smartwatch will be used.

3.5.3 Dashboard Overview and Compliance Scoring

The central feature of our application's UI is the Dashboard, which provides users with a compliance percentage derived from the proportion of checklist items that meet the specified regulatory standards, based on the chosen regulations and the particular smartwatch models being evaluated. This percentage reflects the number of questions answered positively out of the total. The percentage is color-coded for intuitive understanding: red indicates a compliance percentage below 60%, signifying a high risk to privacy or security; orange indicates a compliance percentage between 60% and 80%, suggesting caution is needed; and green indicates a compliance percentage above 80%, representing a secure status. Additionally, the dashboard provides clear and concise explanations of the reasons for the deductions, offering users transparent and actionable insights.

3.5.4 Detailed Reporting

The Detailed Report section delves into the specifics behind the dashboard's summary, offering users a comprehensive view of their smartwatch's compliance with privacy and security standards. This layout shows each question from the compliance checklist and indicates whether the connected smartwatch meets ('yes' in green) or does not meet ('no' in red) these standards. This report not only informs users of potential risks but also empowers them with knowledge about their device's privacy and security posture. The layout is crafted to facilitate easy understanding, and color-coded issues for straightforward navigation and action.

3.5.5 User Feedback

Recognizing the value of user insights and the need for continuous improvement, the User Feedback section provides a simple yet effective way for users to communicate directly with the development team. Here, users can report functionality issues, suggest enhancements, offer general feedback about their experience, or

simply rate the application from 1 to 5 stars (5 stars indicates perfect and 1 star indicates extremely poor performance). This feedback form is designed to be user-friendly, encouraging even those less technically inclined to share their thoughts.

3.5.6 Device Management

Finally, the Connect to Other Device feature addresses the practical needs of users who may own multiple smartwatches or wish to monitor devices for several children. This section of the UI simplifies the process of adding and managing multiple devices, ensuring the app remains a tool for families or individuals with more than one smartwatch. The design allows quick pairing and swapping between devices without navigating through complex settings, making it straightforward for users to manage the privacy and security compliance of all their smartwatches efficiently.

3.5.7 Navigational Elements

The application's design incorporates a Navigation Bar at the bottom of the screen, designed for ease of use and quick access to the app's core sections. This navigational tool enhances the user experience by offering one-tap access to: the Dashboard, where the primary compliance percentage and alerts are displayed; the Detailed Report, which provides an in-depth analysis of compliance issues; the User Feedback form, encouraging user interaction and feedback; and the Connect to Other Device feature, allowing for seamless management of multiple smartwatches. This navigation bar tries to help users effortlessly explore the full range of functionalities offered.

The flow diagram 3.4 visualizes the overall design, illustrating the interactions between different components of the system, from user interaction to detailed compliance insights.

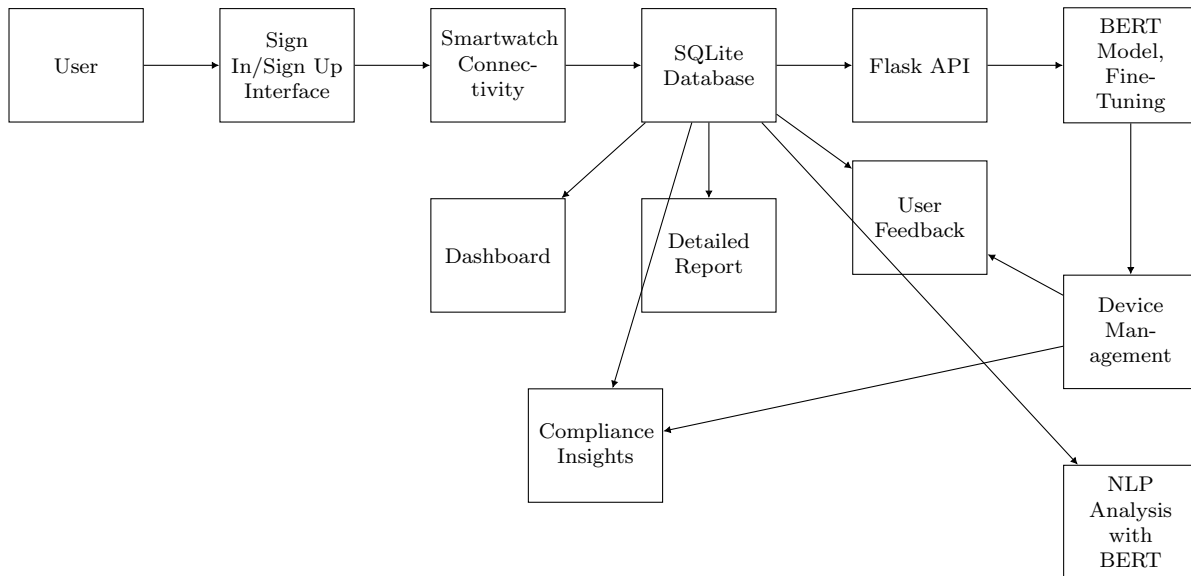


Figure 3.4: Flow Diagram Of Automated Compliance Checking System Design

The design of the Automated Compliance Checking application integrates advanced NLP techniques with a user-friendly interface to ensure the privacy and security compliance of smartwatches intended for children.

Chapter 4

Implementation

This chapter describes the implementation of the application prototype for evaluating the compliance of smartwatches. The system integrates several core components: a relational database for data management, a RESTful API for seamless interaction, an automated compliance checking mechanism utilizing NLP, and Android Studio to build the application. This chapter details the implementation steps and technologies used.

4.1 Database Implementation

The implementation of the database schema involved setting up the SQLite database within the Android Studio environment. For the privacy policies, they were first extracted from the watches' official websites [75, 76] and then transferred into a JSON file format. Checklist and policy data are stored and loaded in JSON format to SQLite.

4.2 NLP Implementation

Various steps for implementing NLP technique were involved here. Including data preparation, data pre-processing, data modeling and evaluation.

4.2.1 Data Splitting

The dataset was split into three subsets to facilitate training, validation, and testing of the BERT model. The training set is used to teach the model, enabling it to learn patterns for predicting the compliance check result; the validation data is important for tuning hyperparameters and test data provides an unbiased evaluation of the model's performance.

- **Training Set:** 70% of the data.
- **Validation Set:** 15% of the data.
- **Test Set:** 15% of the data.

4.2.2 Data Augmentation

To enhance the robustness of the model, data augmentation techniques were applied. Here three specific augmentation methods are used: synonym augmentation (SynonymAug), random word swapping (RandomWordAug), and random word deletion (RandomWordAug). The SynonymAug method replaces words with their synonyms from WordNet, a large lexical database of English [79]. It enhances the dataset with semantically similar sentences. RandomWordAug with the "swap" action randomly swaps words in the sentence, creating new variations and introducing syntactic diversity. RandomWordAug with the "delete" action randomly deletes words from the sentence, helping the model become resilient to missing information. These augmentation techniques collectively improve the model's ability to generalize by exposing it to a wider range of sentence structures and variations, making it more robust.

4.2.3 Model Fine-Tuning

The fine-tuning phase involved loading the pre-trained BERT model as a base, by fine-tuning it on the policies and compliance checklists dataset, which led to improved accuracy and performance:

Table 4.1 sets up the training arguments for fine-tuning the BERT model using the TrainingArguments class from the Hugging Face library for its comprehensive set of tools and pre-trained models. Key parameters include the number of training epochs, batch sizes for training and evaluation, and the number of warmup steps. The warmup steps gradually increase the learning rate at the beginning of training to stabilize the optimization process, while the weight decay helps regularize the model by penalizing large weights, thereby reducing the risk of overfitting. The learning rate is set to $2e-5$, with a weight decay of 0.01 to prevent overfitting.

Table 4.1: Training Arguments

| Argument | Value |
|-----------------------------|--------|
| num_train_epochs | 10 |
| per_device_train_batch_size | 32 |
| per_device_eval_batch_size | 32 |
| warmup_steps | 1000 |
| weight_decay | 0.01 |
| logging_steps | 10 |
| learning_rate | $2e-5$ |

4.2.4 Model Evaluation

The evaluation phase involved assessing the performance of the fine-tuned BERT model.

A plot of the training and validation loss over each epoch was plotted to evaluate the performance of the fine-tuning process, which helped in assessing the model's learning process, identifying overfitting or underfitting by comparing the trends in training and validation losses across epochs.

After that, the fine-tuned model was evaluated on a test dataset using the `trainer.evaluate` method from the Hugging Face library to compute evaluation metrics and print the results. It then used `trainer.predict` to obtain model predictions on the test set. The true labels were stored in `test_data['answer']`, which computes key performance metrics: overall accuracy indicating the proportion of correct predictions, precision measuring the correctness of positive predictions, recall indicating the ability to identify all positive instances, and F1-score presenting a balance between precision and recall as described in section 5.1.

The evaluation for each checklist was also carried out, to see which one has better performance as described in section 5.2.

4.3 API Implementation

Implementing the Flask API was a critical step in enabling seamless communication between the Android application and the Python server for NLP analysis. The API was designed to handle various requests essential for the functionality of the compliance checking system.

4.3.1 API Endpoints and Functionality

The Flask endpoint was defined to handle POST requests, extract and log JSON data, and retrieve policy and checklist from the request.

As seen in code snippet 4.1, for each question in the checklist, it concatenated the policy text and question, tokenized the combined input, and processed it through the BERT model to obtain predictions. The prediction was interpreted as a prediction of 1 indicating compliance (result set to 1), and any other prediction indicating non-compliance or not mentioned (result set to 0). The compliance results for all questions are compiled into a list, returned as a JSON response, and sent back to Andriod Studio.

```
1 compliance_results = []  
2 for question in checklist:  
3
```

```
4     combined_input = f"{policy_text} {tokenizer.sep_token} {  
5         question}"  
6     inputs = tokenizer(combined_input, return_tensors="pt",  
7         max_length=512, truncation=True, padding="max_length")  
8     outputs = model(**inputs)  
9     prediction = torch.argmax(outputs.logits, dim=1).item()  
10    result = 1 if prediction == 1 else 0  
11    compliance_results.append({"question": question, "answer":  
12        result})  
13 result = {  
14     "compliance_result": compliance_results  
15 }
```

Listing 4.1: Compliance Check Processing with BERT

4.4 User Interface Implementation

The UI of the compliance checking system is implemented to provide an intuitive experience for users, enabling them to get the compliance results effortlessly.

4.4.1 Sign-In and Smartwatch Connectivity

The initial phase of the user interface implementation involved developing the Sign-In/Sign-Up interface and smartwatch connectivity features.

Sign-In/Sign-Up Interface

A clean and intuitive interface was developed using Android Studio's XML layout design. This includes text fields for email and password, buttons for signing in or signing up, and error messages for invalid inputs as seen in Figure 4.1, it allowed users to access the main features of the application immediately after logging in, without the need to reconnect with their smartwatches each time, which streamlined the user experience and saving time.

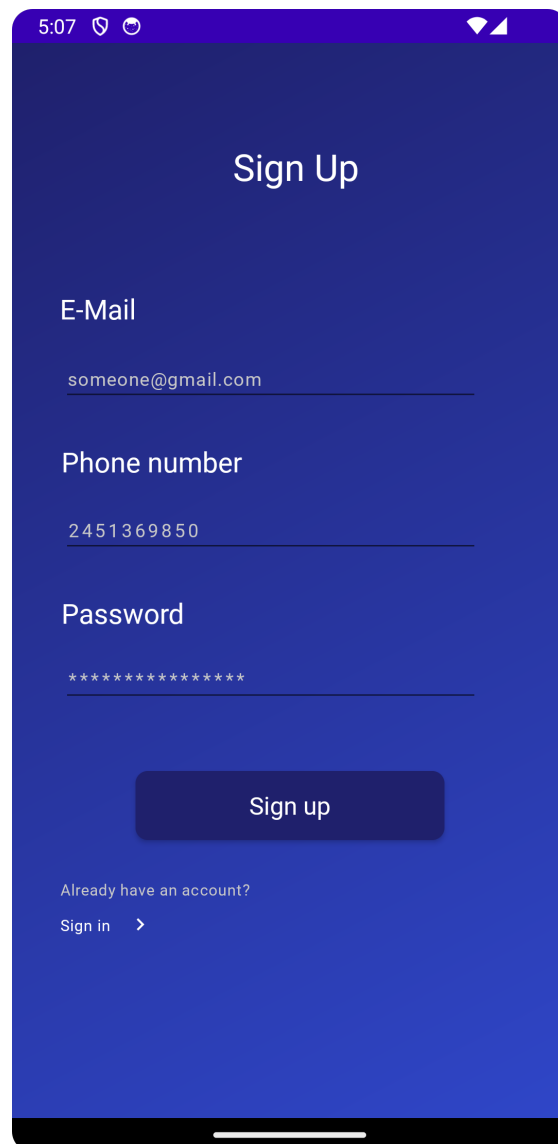


Figure 4.1: Sign-In/Sign-Up Interface

Smartwatch Connectivity

The function shows the watches' names and picture, presenting on-screen instructions through Android's `ConstraintLayout` and `TextView` components to guide users. The `Connection Handling` component develops logic to list devices, using `RecyclerView` to display the list of devices and handle user selection efficiently, as seen in Figure 4.2.

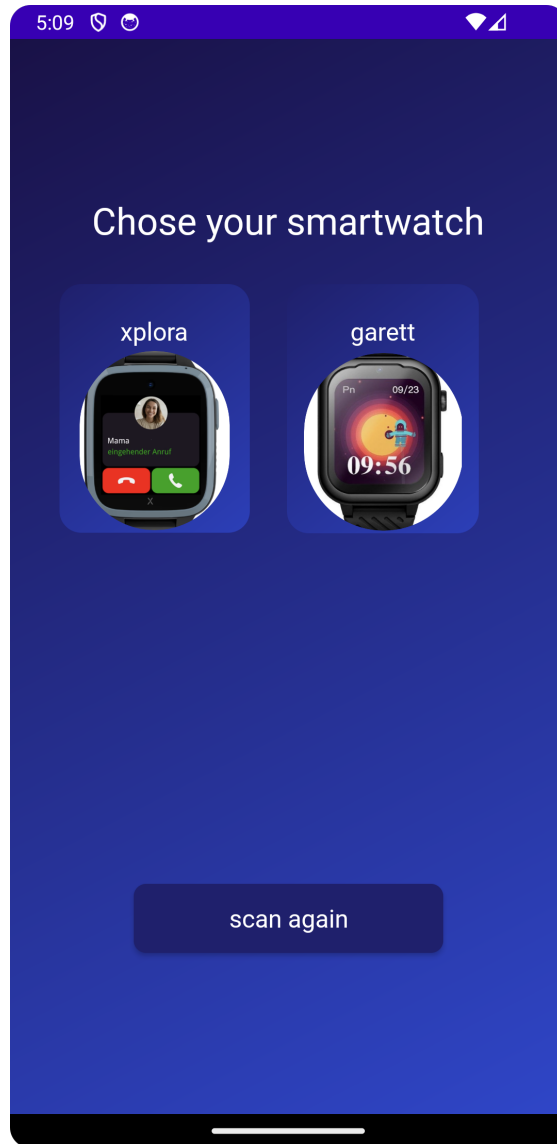


Figure 4.2: Smartwatch Connectivity Interface

Area Selection Implementation

The Area Selection feature is implemented to allow users to choose their geographical region, ensuring that the compliance results are based on the specific regulations applicable in that area. This was achieved using a dropdown menu that lists various regions such as the EU, USA, China, Switzerland, and South Africa as seen in Figure 4.3. The selected region was then used to filter and apply the relevant regulatory criteria to the compliance analysis.

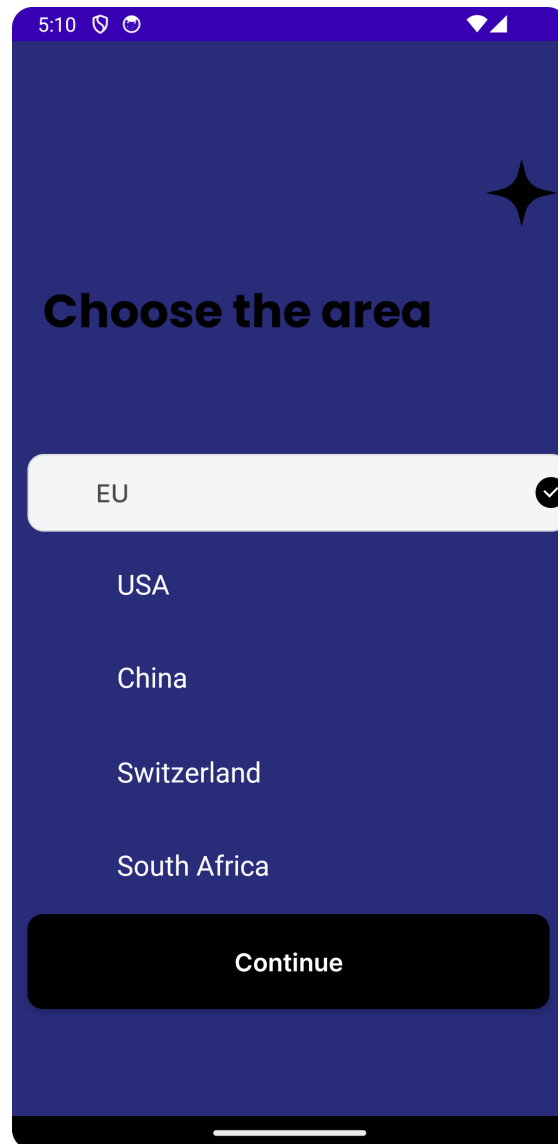


Figure 4.3: Area Selection Screen

4.4.2 Dashboard Overview and Compliance Result

The Dashboard is the central feature of the application's UI, providing users with an immediate compliance percentage along with a number of compliant questions in total, based on their selected regulations and smartwatches.

A dynamic dashboard was developed using Android's CardView and TextView components to prominently display the compliance score, implementing logic to color-code the compliance percentage based on predefined thresholds (red for below 60%, orange for 60-80%, and green for above 80%) using Android's Color class. Additionally, add sections to the dashboard to provide clear and concise explanations for scores below 80%, utilizing ListView to display multiple deductions as seen in Figure 4.4.

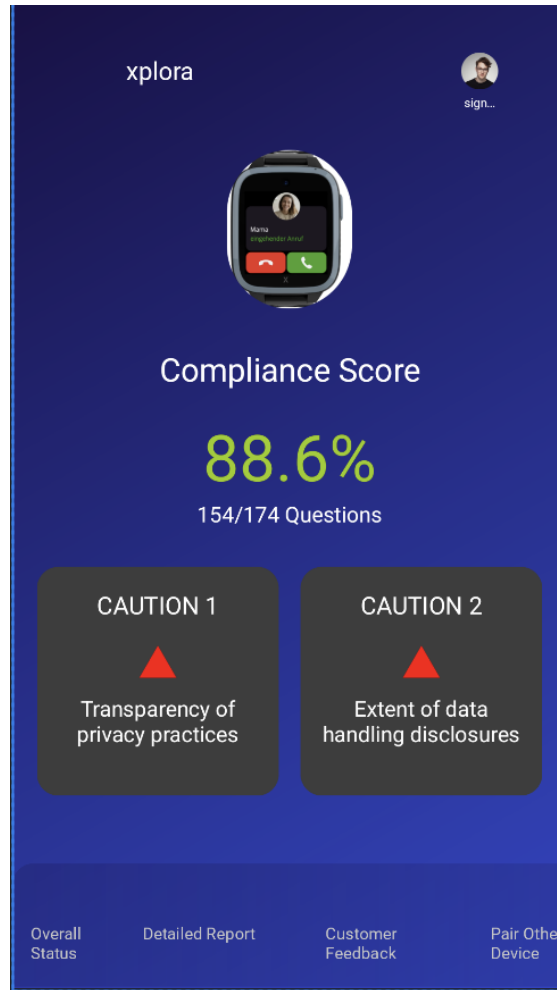


Figure 4.4: Dashboard Interface

4.4.3 Detailed Reporting

The Detailed Report section offered the whole checklist and the answers to the smartwatch's compliance with privacy. It provided users with more detailed information about which aspect the watch is not compliant with, enabling users to identify and understand the precise areas of non-compliance.

A detailed report layout was implemented using `ScrollView` and `LinearLayout` to list each compliance criterion, and color-coded yes/no was used to indicate whether each criterion is met or not met. Additionally, the detailed report was organized into categories for easy navigation, using `ExpandableListView` to allow users to expand and collapse sections as seen in Figure 4.5.

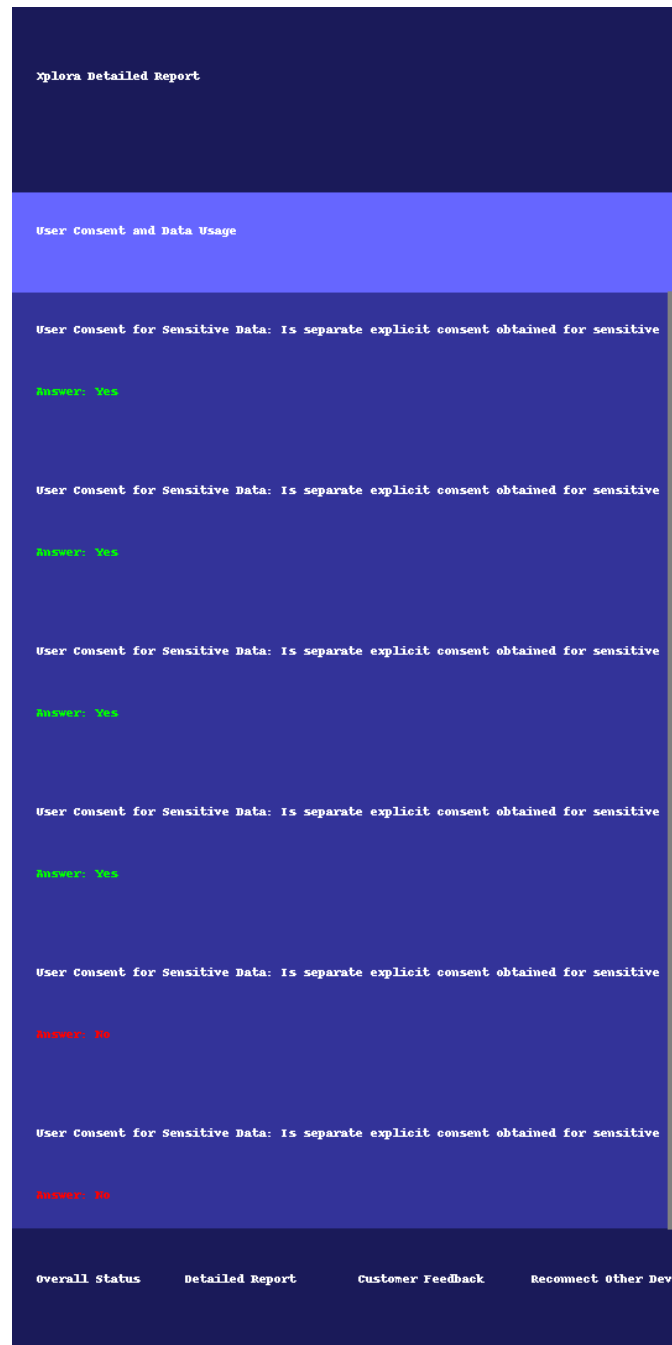


Figure 4.5: Detailed Reporting Interface

4.4.4 User Feedback

The User Feedback section allowed users to communicate directly with the development team.

A simple feedback form was created using a rating bar with Stepsize 1 and EditText for input fields and a Button for submission as seen in Figure 4.6, ensuring user-friendliness by providing placeholders and hints.

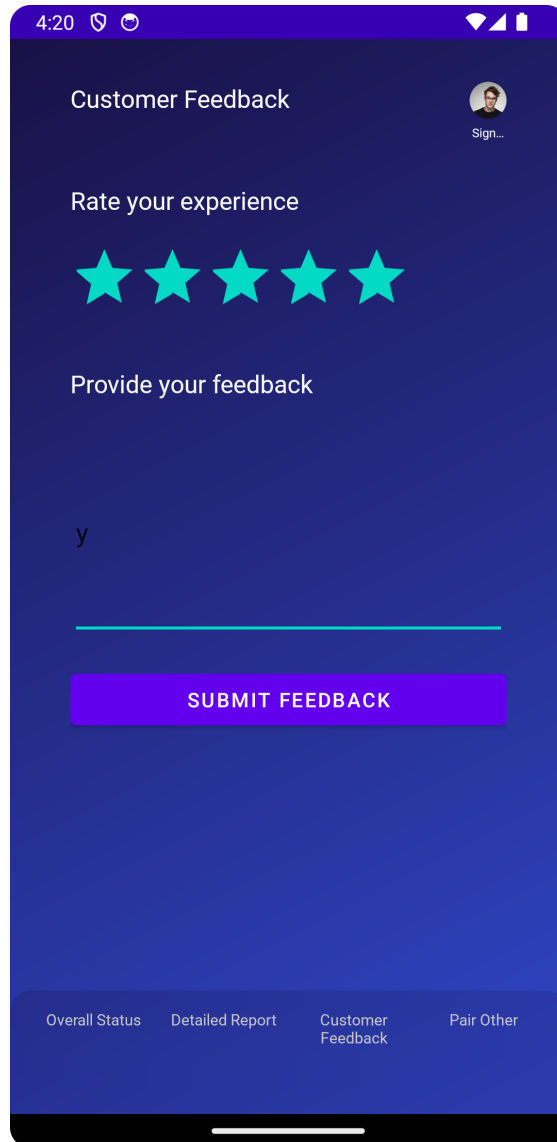


Figure 4.6: User Feedback Interface

4.4.5 Multiple Device Management

An interface was developed to list multiple devices using RecyclerView as seen in Figure 4.7, enabling users to add and manage smartwatches easily. Implemented logic for quick pairing and swapping between devices using Android's SharedPreferences to store paired device information.

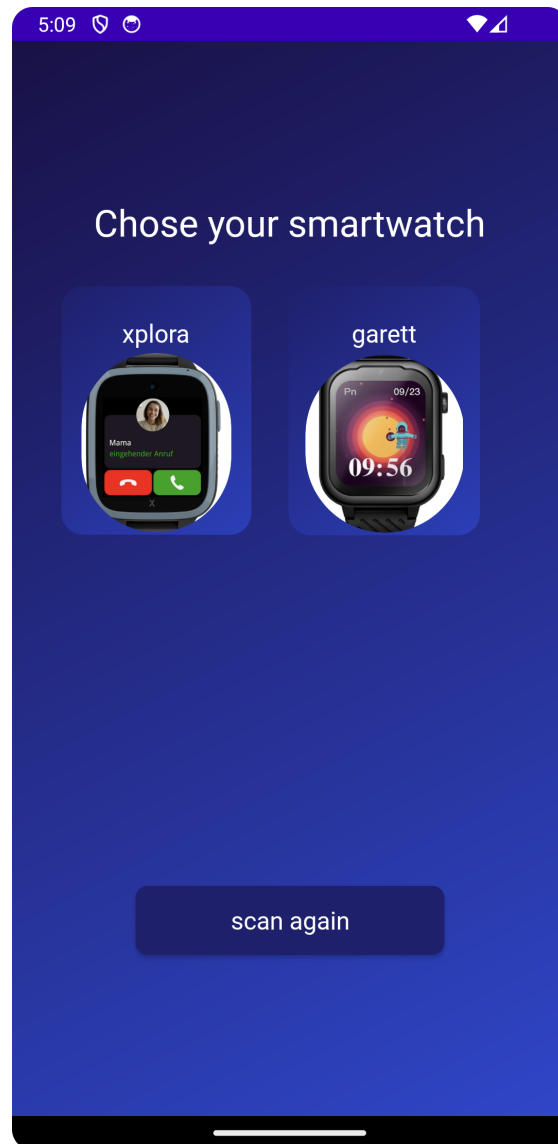


Figure 4.7: Device Management Interface

4.4.6 Navigational Elements

A bottom navigation bar was implemented using Android's BottomNavigationView at the bottom of each layout: Dashboard, Detailed Report, User Feedback, and Connect to Other Device. Utilized FragmentManager to switch between different sections of the app, maintaining a smooth user experience as seen in Figure 4.8.

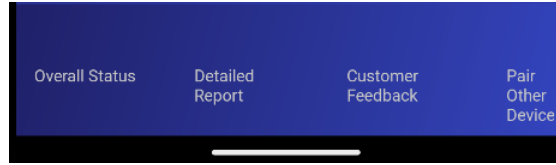


Figure 4.8: Navigation Bar

This implementation ensured the application for evaluating the compliance of smartwatches, integrating database management, NLP techniques, and a user-friendly interface, to provide accurate and accessible compliance information to users.

Chapter 5

Evaluation

The evaluation of the Automated Compliance Checking application has several critical aspects, including the performance of the NLP model, the performance of the compliance checking framework on the five regulatory guidelines, a comparative analysis with similar approaches, and the evaluation comparing the chosen watches: Xplora and Garrett.

5.1 NLP Model Evaluation

Figure 5.1 shows the training and validation loss over 50 epochs. The training loss (blue line) decreases rapidly and stabilizes around a lower value after approximately 10 epochs, indicating that the model is effectively learning from the training data. The validation loss (orange line) also drops quickly, stabilizing around the same point, which suggests that the model maintains good performance on unseen data without significant overfitting or underfitting.

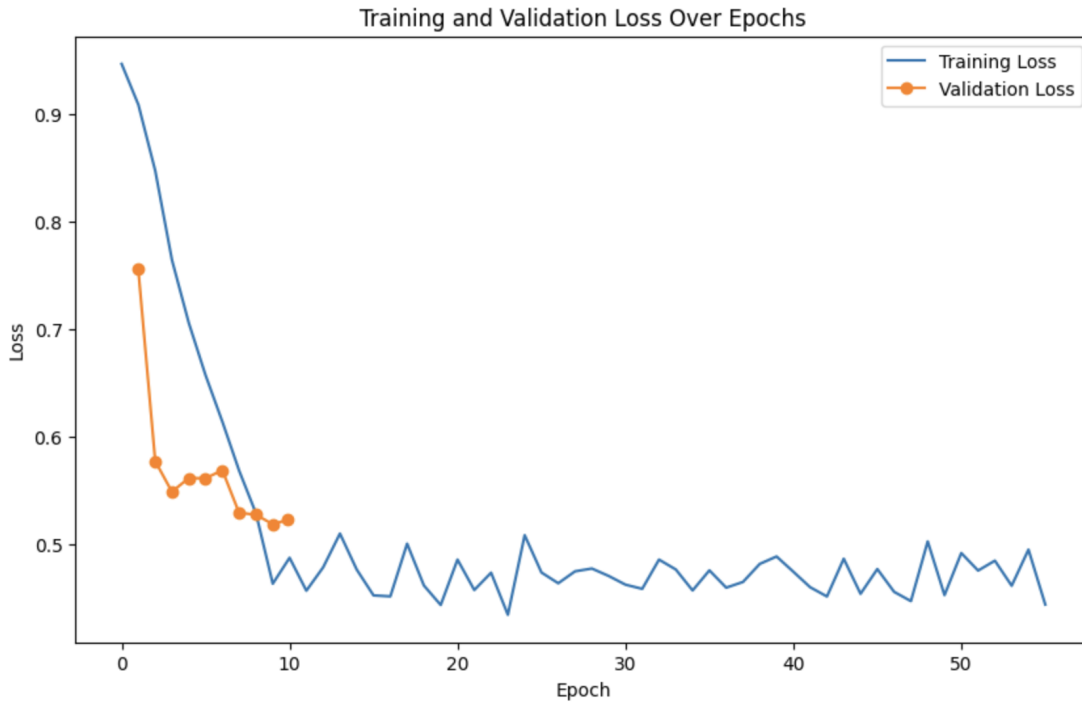


Figure 5.1: Training and validation loss

For the fine-tuning process, two approaches were utilized: The first approach was adjusting parameters. Table 5.1 shows the evaluation results from these processes.

Table 5.1: Evaluation metrics for different learning rates and epochs

| Weight Decay | Epochs | Accuracy | Precision | Recall | F1-Score |
|--------------|--------|----------|-----------|--------|----------|
| 0.001 | 5 | 0.75 | 0.73 | 0.72 | 0.72 |
| 0.001 | 10 | 0.78 | 0.76 | 0.75 | 0.75 |
| 0.01 | 5 | 0.80 | 0.78 | 0.77 | 0.77 |
| 0.01 | 10 | 0.82 | 0.80 | 0.82 | 0.81 |

The second is changing methods (such as using different augmentation techniques). Table 5.2 shows the evaluation results from it.

Table 5.2: Evaluation Metrics for Different Augmentation Techniques

| Augmentation Technique | Accuracy | Precision | Recall | F1-Score |
|--|----------|-----------|--------|----------|
| Synonym Augmentation | 0.80 | 0.78 | 0.77 | 0.77 |
| Add RandomWordAug with "swap" | 0.80 | 0.81 | 0.80 | 0.80 |
| Add RandomWordAug with "delete" | 0.63 | 0.62 | 0.61 | 0.62 |
| Add RandomWordAug with "swap" and "delete" | 0.82 | 0.81 | 0.82 | 0.82 |

After fine-tuning, the model was evaluated using standard metrics to assess its performance in classifying compliance criteria. The evaluation metrics include ac-

curacy, precision, recall, and F1-score. Accuracy measures the overall proportion of correctly classified predictions, including both compliant and non-compliant answers, out of the total instances evaluated. Precision focuses on the accuracy of positive predictions, specifically the proportion of true compliant answers among all answers predicted as compliant. Recall, on the other hand, measures the proportion of actual compliant answers that were correctly identified by the model. The F1-score provides a single metric that balances precision and recall by calculating their harmonic mean, giving an overall sense of the model’s performance in identifying compliant answers accurately. These metrics were calculated on the test set, which comprised 15% of the entire dataset.

Table 5.3 shows the model’s overall accuracy is 80%, indicating a high level of correctness in classifying the compliance criteria. It achieved a precision of 82.3%, reflecting its ability to minimize false positives in compliance classification. The recall was measured at 80.2%, showing the model’s effectiveness in identifying true positives. The F1-score was 80%, providing a balanced measure of the model’s precision and recall capabilities.

Table 5.3: Evaluation metrics for the fine-tuned model

| Metric | Value |
|---------------|--------------|
| Accuracy | 82% |
| Precision | 81.2% |
| Recall | 82% |
| F1-Score | 81.6% |

These results indicate that the fine-tuned BERT model achieved high performance across all metrics, demonstrating its effectiveness in accurately classifying compliance criteria within regulatory checklists and privacy policies.

5.2 Regulatory Guidelines Evaluation

The system’s efficacy was evaluated against five comprehensive regulatory guidelines: GDPR, CPRA, PIPL, nFADP, and POPIA. Each regulatory guideline presented distinct requirements and criteria for compliance.

This result 5.4 shows a relatively high outcome for GDPR, CCPA and nFADP of 83.7%, 81.5%, and 71.1% in F1-Score respectively, reflecting the model’s good performance in handling well-established and comprehensive regulations. For PIPL and POPIA, the lower success rates of 27.4% and 41.6% in F1-Score suggest the need for improvement, it might be because these two regulations differ significantly from Western data protection laws.

Table 5.4: Metrics for checklist evaluation across various compliance regulations.

| Compliance Regulation | Accuracy | Precision | Recall | F1-Score |
|-----------------------|----------|-----------|--------|----------|
| GDPR | 0.765 | 0.669 | 0.745 | 0.714 |
| CCPA | 0.833 | 1.000 | 0.833 | 0.909 |
| PIPL | 0.846 | 0.874 | 0.846 | 0.828 |
| nFADP | 0.889 | 0.926 | 0.889 | 0.896 |
| POPIA | 0.800 | 1.000 | 0.800 | 0.889 |

As the F1-Score for GDPR is relatively lower, so training data for GDPR was augmented again as described in section 3.3.3. Table 5.5 shows an increase for GDPR, with a 76.5% of F1-Score.

Table 5.5: Final Metrics for checklist evaluation across various compliance regulations

| Compliance Regulation | Accuracy | Precision | Recall | F1-Score |
|-----------------------|----------|-----------|--------|----------|
| GDPR | 0.765 | 0.765 | 0.765 | 0.765 |
| CCPA | 0.833 | 1.000 | 0.833 | 0.909 |
| PIPL | 0.923 | 0.931 | 0.923 | 0.920 |
| nFADP | 0.889 | 0.926 | 0.889 | 0.900 |
| POPIA | 0.800 | 1.000 | 0.800 | 0.889 |

There is also an increase for the model, with an 84.6% F1-Score and 85.5% precision, as shown in Table 5.6.

Table 5.6: Evaluation metrics for the final fine-tuned model

| Metric | Value |
|-----------|-------|
| Accuracy | 84% |
| Precision | 85.5% |
| Recall | 84% |
| F1-Score | 84.6% |

5.3 Evaluation on Specific Smartwatch Models: Xplora and Garrett

The practical application of the compliance checking application was evaluated using two specific smartwatch models: Xplora and Garrett. We here manually deduct some questions labeled as 0, which cannot be determined by policy (e.g., "Do you ensure consent choices are displayed equally without using nudging or dark patterns?", from the checklist (see appendix 3)).

5.3.1 Garrett Smartwatch

The Garrett smartwatch achieved a compliance percentage of 70.4%, with 112 out of 159 questions answered as compliant. This suggests a generally secure and privacy-compliant status for the device.

Specifically, the smartwatch showed notable strengths in areas related to Data Management and Rights, where it achieved 27 compliant answers out of 29 as shown in Table 5.7, indicating robust data handling and user rights practices.

Table 5.7: Example checklist questions for Garrett: Performance on Data Management and Rights

| Question | Answer |
|---|--------|
| Do you provide at least two contact options, such as a toll-free phone number, web form, or email, for consumers to reach you? | 1 |
| Have you set up a system to enable the submission of Data Subject Access Requests (DSARs) allowing consumers to verify their identity and residency? | 1 |
| Have you set up a system to enable submissions for verification requests, explaining why a request could not be verified and allowing consumers to rectify? | 1 |
| Do you keep track of all Data Subject Access Requests (DSARs) and your business responses? | 0 |

However, there were areas identified for improvement, particularly concerning User Consent and Data Usage, where only 16 out of 28 answers were compliant as shown in Table 5.8.

Table 5.8: Example checklist questions for Garrett: Performance on: User Consent and Data Usage

| Question | Answer |
|--|--------|
| Do you obtain granular consent for individual purposes, not bundling consent with other purposes or activities? | 0 |
| Do you make it easy to withdraw consent, with changing consent or opting out as easy as opting in? | 1 |
| Do you ensure nonessential cookies and other tracking technologies are not triggered or loaded until valid user consent has been obtained? | 0 |
| Do you ensure that nonconsenting users cannot be blocked entirely but can be notified about the effects on functions or services? | 0 |

Additionally, the Advertising and Tracking category also didn't perform well, with only 5 out of 13 questions being compliant as seen in Table 5.9.

Table 5.9: Example checklist questions for Garrett: Performance on: Advertising and Tracking

| Question | Answer |
|--|--------|
| Do you ensure users have the option to grant or withdraw consent for each purpose? | 0 |
| Do you obtain users' voluntary and informed consent to store cookies on their device(s)? | 1 |
| Do you ensure that no cookies are loaded until users have given consent? | 0 |
| Have you enabled consumers to exercise rights, like opting out, via a banner or pop-up when users visit your site, e.g., with a Consent Management Platform? | 0 |

These gaps suggest that while the device meets many regulatory standards, there are significant areas where it could improve, particularly in ensuring clearer user consent mechanisms and more transparent advertising and tracking practices.

5.3.2 Xplora Smartwatch

The Xplora smartwatch achieved a compliance percentage of 88.7%, with 141 out of 159 questions answered as compliant, indicating overall strong adherence to privacy and security standards but also highlighting areas for improvement.

The device excelled in Consent and Data Usage, achieving a perfect compliance score of 20 out of 20, reflecting robust practices in user consent and data management as detailed in table 5.10.

Table 5.10: Example checklist questions for Xplora: Performance on: User Consent and Data Usage

| Question | Answer |
|---|--------|
| Do you enable consumers to exercise their rights, such as opting out, via a banner or pop-up when they visit your site? | 1 |
| Have you informed users about their right to opt-out of the sale or sharing of their personal data? | 1 |
| Do you re-offer opt-in consent to consumers who have opted out, presenting the option to opt-in again after 12 months? | 1 |
| Do you provide a "Limit The Use of My Sensitive Personal Information" link to enable opt-out? | 1 |

However, significant deficiencies were found in the area of children's safety, where only 1 compliant out of 6, underscoring a critical area for enhancement as outlined in table 5.11.

5.3. EVALUATION ON SPECIFIC SMARTWATCH MODELS: XPLORA AND GARETT45

Table 5.11: Example checklist questions for Xplora: Performance on: Children’s Safety

| Question | Answer |
|---|--------|
| Have you obtained consent from a parent or guardian before collecting personal data from children? | 1 |
| Do you assess and obtain consent from parents or guardians for processing personal information of minors under 14? | 0 |
| Do you establish specialized processing rules for minors’ data? | 0 |
| Are you processing any sensitive personal information in China such as biometric characteristics, religious beliefs, medical health, financial accounts, or information of minors under 14? | 0 |

Xplora generally upholds privacy and security standards, there are significant gaps, particularly concerning measures to protect children’s safety.

Table 5.12 shows the whole performance of five categories between Xplora and Garrett, Xplora is better in User Consent and Data Usage, Data Management and Rights, and Privacy Policies and Practices Data Handling; while Garrett is better at Children’s Safety, and Advertising and Tracking.

Table 5.12: Performance of Xplora and Garrett in Different Categories

| Category | Xplora | Garrett |
|--|-----------|-----------|
| User Consent and Data Usage | 100%(32) | 43.8%(14) |
| Data Management and Rights | 96.8%(30) | 93.5%(29) |
| Privacy Policies and Practices Data Handling | 91.7%(55) | 70.0%(42) |
| Children’s Safety | 14.3(1)% | 57.1%(4) |
| Advertising and Tracking | 24.1%(7) | 41.2%(12) |

Table 5.13 shows Xplora has the best performance in GDPR, worst performance in PIPL; while Garrett performed better in CCPA, but did worse in GDPR.

Table 5.13: Performance of Xplora and Garrett in Different Regulations

| Regulation | Xplora | Garrett |
|------------|--------|---------|
| GDPR | 97.9% | 53.3% |
| CCPA | 87.5% | 91.3% |
| PIPL | 67.6% | 67.6% |
| nFADP | 92.3% | 81.6% |
| POPIA | 93.3% | 65.5% |

5.4 Comparative Analysis with Similar Approaches

A comparative analysis was conducted to benchmark the performance of the Automated Compliance Checking system against similar approaches in the domain of regulatory compliance checking.

5.4.1 Traditional Manual Auditing

Traditional methods involve manual auditing by legal experts, which are time-consuming and prone to human error. In contrast, the automated system in this thesis provided faster compliance checks, significantly reducing the auditing time and enhancing accuracy. This aligns with the findings by Odonkor et al. (2024), which emphasize that AI-driven systems offer notable improvements in accuracy and efficiency over manual processes [80]. This comparison shows the benefits of automation in streamlining regulatory compliance.

5.4.2 Other NLP-Based Systems:

Compared to other NLP-based systems, for the task of Categories Prediction, the fine-tuned BERT model in this thesis achieved an F1-score of 84.6%, outperforming the best-reported performance of 73 by the T5 (Text-to-Text Transfer Transformer) model with individual fine-tuning in the referenced study [81]. For another paper [82], performance was improved by implementing the Semantic Role-Based Representation (DERECHA) process, which involves creating detailed semantic frames that represent the roles and relationships in GDPR requirements and matching them with corresponding elements in Data Processing Agreement (DPA) statements. This method attains a precision of 89.1% and a F1-Score of 85.7%, attributed to the inclusion of Defining Semantic Frames (SFs), which provides a structured representation of sentences by breaking them down into events (predicates) and their participants (arguments with specific semantic roles). This method was not chosen in this thesis because constructing detailed semantic frames for each requirement, manually annotating DPA statements, and continuously updating the system to reflect legal changes require expert involvement. This thesis focuses more on achieving practical and interpretable results.

5.5 Summary of Evaluation

The evaluation of the Automated Compliance Checking system highlights its effectiveness in providing accurate and consistent compliance assessments across various regulatory frameworks and specific smartwatch models. Integrating advanced NLP techniques with a user-friendly interface facilitated effective user engagement and reliable compliance insights.

The high performance of the BERT model, along with a comprehensive compliance framework, underscores the system’s potential as a valuable tool for enhancing data privacy and security compliance in children’s smartwatches.

Despite these strengths, several limitations and challenges exist. Fine-tuning the BERT model on policy texts may not fully capture the nuances and context-specific details required for comprehensive compliance checks. Policy language can be complex, and variations in interpretation can lead to discrepancies in compliance evaluations. For example, GDPR has a lower F1-score, which could be because GDPR is known for its broad scope, covering a wide range of data protection aspects. This complexity can make it more challenging to model accurately capture all compliance aspects. Additionally, the accuracy of the model heavily depends on the quality and representativeness of the training data. Limited access to diverse and high-quality policy and regulatory documents can constrain the model’s ability to generalize across different policies and regulations.

There is significant potential for expanding and improving the system. Enhanced data collection, including a wider variety of regulatory documents such as international regulations and sector-specific regulations, can improve the model’s generalization capabilities. To address the challenge of text understanding, employing advanced techniques such as multi-task learning can be beneficial [83], which allows the model to learn from multiple related tasks, thereby improving its ability to understand and interpret complex regulatory language.

In summary, while the Automated Compliance Checking application demonstrates high accuracy and practical applicability, addressing its limitations and challenges through targeted improvements can further enhance its effectiveness and foster wider adoption in the field of regulatory compliance.

Chapter 6

Final Considerations

6.1 Summary

This thesis focused on developing an automated compliance checking application for children’s smartwatches, ensuring adherence to various privacy regulations, including GDPR, CPRA, nFADP, PIPL, and POPIA. The thesis successfully integrated advanced NLP techniques to analyze and evaluate privacy policies and regulatory documents accurately. The paper successfully met its general and specific objectives by effectively automating the compliance checking process, which reduced the effort required for manual audits while ensuring consistent and reliable compliance checks. Each smartwatch model evaluated demonstrated varying levels of compliance, underscoring the system’s capability to accurately assess different regulatory requirements and providing insights into the compliance landscape of various smartwatch models.

There are several factors that contribute to the successful achievement of these objectives. The integration of NLP techniques, specifically the BERT model, ensured accurate interpretation and analysis of privacy policies and regulatory documents. The development of a comprehensive compliance framework, based on legal research and supplementary online resources, provided a robust foundation for automated checks. Additionally, the user-friendly interface, designed in Android Studio, facilitated easy interaction for users, enhancing engagement and usability.

6.2 Conclusions

The model demonstrates an overall performance of 80% in F1-Score for compliance checking, with a particularly high F1 score for regulation CCPA (0.909), PIPL (0.920), and nFADP(0.900). However, it shows a lower F1 score for GDPR (0.765), indicating a need for further refinement. When compared to traditional

manual auditing methods and other NLP-based systems, our model offers faster and relatively accurate performance.

For the two evaluated watches Xplora and Garrett, Xplora exhibits superior overall performance with an 88.7% compliance percentage, especially in adhering to GDPR, CCPA, POPIA, and nFADP regulations, while relatively median performance for PIPL, which could indicate Xplora’s main focus in Europe and America market than Asian market. It excels in aspects such as consent and data usage, data management and rights, and privacy policies and practices. This focus can be attributed to Xplora’s intention to build trust and reliability among consumers in these regions by ensuring robust data protection measures and adherence to privacy laws; While Garrett has a relatively lower overall performance with a percentage of 70.4%, however it performs better in compliance with CCPA which can indicate its main market focus in America and excels in aspects related to children’s safety, advertising, and tracking. Garrett’s performance in these areas demonstrates a commitment to addressing the privacy concerns prevalent in the American market, such as protecting children’s data and ensuring transparency in advertising and tracking practices.

6.3 Future Work

Future work could focus on enhancing model accuracy, particularly for GDPR, which is known for its comprehensive and detailed data protection requirements. The broad scope and unique aspects of this regulation require further refinement of the model, including fine-tuning the algorithm and expanding the training datasets to better capture the specific nuances of GDPR compliance.

Another area of focus is expanding the scope of compliance checks. Including more smartwatch models and additional privacy regulations such as Japan’s Act on the Protection of Personal Information (APPI) and Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), will enhance the application’s utility for international markets and broaden the application’s applicability. By doing so, the compliance check framework can offer a more comprehensive assessment across various devices and legal frameworks.

In addition, integrating real-time data feeds, such as using Nmap for network security assessments, and tools like Wireshark which can analyze network traffic in detail, can significantly enhance the system’s capabilities by enabling dynamic compliance checking and providing up-to-date insights into potential vulnerabilities and compliance status. However, implementing this feature requires substantial engineering efforts, particularly due to challenges related to encryption and privacy concerns, as many devices encrypt data to protect user information. So due to the complexity of ensuring data security and the legal implications of intercepting encrypted data, this integration is beyond the current scope of this thesis.

By addressing these areas, future research can build on the foundation laid by this thesis and can be helpful for guardians and help to build a safer environment for children to grow up.

Bibliography

- [1] M. Masoumian Hosseini, S. T. Masoumian Hosseini, K. Qayumi, S. Hosseinzadeh, and S. S. Sajadi Tabar, “Smartwatches in healthcare medicine: assistance and monitoring; a scoping review,” *BMC Medical Informatics and Decision Making*, Vol. 23, No. 1, p. 248, 2023.
- [2] J. W. Kim, J. H. Lim, S. M. Moon, H. Yoo, and B. Jang, “Privacy-preserving data collection scheme on smartwatch platform,” *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2019, pp. 1–4.
- [3] “California Consumer Privacy Rights Act (CCPA),” <https://oag.ca.gov/privacy/ccpa>, 2020, accessed: yyyy-mm-dd.
- [4] “Protection of Personal Information Act, 2013 (Act No. 4 of 2013),” <https://www.gov.za/documents/protection-personal-information-act>, 2013, accessed: yyyy-mm-dd.
- [5] “Personal Information Protection Law (PIPL) of the People’s Republic of China,” <http://www.npc.gov.cn/englishnpc/c23934/202108/f6301f6fad2b4dfab9d8f6e3f77a98c8.shtml>, 2021, accessed: yyyy-mm-dd.
- [6] European Parliament and Council of the European Union, “Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation),” <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, 2016, accessed: yyyy-mm-dd.
- [7] “Federal Act on Data Protection (FADP),” <https://www.admin.ch/opc/en/classified-compilation/19920153/index.html>, 2019, accessed: yyyy-mm-dd.
- [8] M. E. Cecchinato, A. L. Cox, and J. Bird, “Smartwatches: the good, the bad and the ugly?” *Proceedings of the 33rd Annual ACM Conference extended abstracts on human factors in computing systems*, 2015, pp. 2133–2138.
- [9] H. J. Smidt and O. Jokonya, “The challenge of privacy and security when using technology to track people in times of covid-19 pandemic,” *Procedia Computer Science*, Vol. 181, pp. 1018–1026, 2021.

- [10] P. A. Zandbergen, “Accuracy of iphone locations: A comparison of assisted gps, wifi and cellular positioning,” *Transactions in GIS*, Vol. 13, pp. 5–25, 2009.
- [11] S. Kumar and K. B. Moore, “The evolution of global positioning system (gps) technology,” *Journal of science Education and Technology*, Vol. 11, pp. 59–80, 2002.
- [12] gov. Gps: The global positioning system. [Online]: <https://www.gps.gov/>
- [13] AEROSPACE. A brief history of gps. [Online]: <https://aerospace.org/article/brief-history-gps>
- [14] L. Árvai, “Application of smartwatches in elderly care with indoor localization functionality.” *Int. J. Interact. Mob. Technol.*, Vol. 15, No. 5, pp. 174–186, 2021.
- [15] Z. Tariq, B. e Zainab, and M. Z. Hussain, “Evaluating the effectiveness and resilience of ssl/tls, https, ipsec, ssh, and wpa/wpa2 in safeguarding data transmission,” *UCP Journal of Engineering & Information Technology*, Vol. 1, No. 2, pp. 01–07, 2023.
- [16] L. Barkhuus and A. K. Dey, “Location-based services for mobile telephony: a study of users’ privacy concerns.” *Interact*, Vol. 3. Citeseer, 2003, pp. 702–712.
- [17] A. J. Biega, P. Potash, H. Daumé, F. Diaz, and M. Finck, “Operationalizing the legal principle of data minimization for personalization,” *Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval*, 2020, pp. 399–408.
- [18] B. Hu, “Wi-fi based indoor positioning system using smartphones,” *School of Mathematical and Geospatial Sciences College of Science, Engineering and Health Royal Melbourne Institute of Technology (RMIT) University*, 2013.
- [19] N. Dinh-Van, F. Nashashibi, N. Thanh-Huong, and E. Castelli, “Indoor intelligent vehicle localization using wifi received signal strength indicator,” *2017 IEEE MTT-S international conference on microwaves for intelligent mobility (ICMIM)*. IEEE, 2017, pp. 33–36.
- [20] Wikipedia contributors, “Received signal strength indicator — Wikipedia, The Free Encyclopedia,” 2024, [Online; accessed 29-July-2024]. [Online]: https://en.wikipedia.org/wiki/Received_signal_strength_indicator
- [21] M. Chelly and N. Samama, “Detecting visibility in heterogeneous simulated environments for positioning purposes,” *IPIN 2010 : International Conference on Indoor Positioning and Indoor Navigation*, Hoenggerberg, Switzerland, Sep. 2010, p. . [Online]: <https://hal.science/hal-01345039>
- [22] C. Kaplanis, “Detection and prevention of man in the middle attacks in wi-fi technology,” Ph.D. dissertation, Aalborg University Aalborg, Denmark, 2015.

- [23] D. S. Bhatti, S. Saleem, A. Imran, Z. Iqbal, A. Alzahrani, H. Kim, and K.-I. Kim, "A survey on wireless wearable body area networks: A perspective of technology and economy," *Sensors*, Vol. 22, No. 20, p. 7722, 2022.
- [24] I. S. Al-Mejibli and N. R. Alharbe, "Analyzing and evaluating the security standards in wireless network: A review study," *Iraqi Journal for Computers and Informatics*, Vol. 46, No. 1, pp. 32–39, 2020.
- [25] M. Cunche, "I know your mac address: targeted tracking of individual using wi-fi," *Journal of Computer Virology and Hacking Techniques*, Vol. 10, pp. 219–227, 2014.
- [26] Safetrax. (2024) Location tracking role of gps cell tower and wifi triangulation. [Online]: <https://www.safetrax.in/blog/location-tracking-role-of-gps-cell-tower-and-wifi-triangulation/#:~:text=Cell%20Tower%20Triangulation%20Tracking%20System,with%20dense%20cell%20tower%20infrastructure>.
- [27] M. A. Spirito, "On the accuracy of cellular mobile station location estimation," *IEEE Transactions on vehicular technology*, Vol. 50, No. 3, pp. 674–685, 2001.
- [28] K. Lin, A. Kansal, D. Lymberopoulos, and F. Zhao, "Energy-accuracy trade-off for continuous mobile device location," *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010, pp. 285–298.
- [29] G. Miller. (2024) Finding you teleco-vulnerabilities for location disclosure. [Online]: <https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/>
- [30] V. Kaul, B. Nemade, V. Bharadi *et al.*, "Next generation encryption using security enhancement algorithms for end to end data transmission in 3g/4g networks," *Procedia Computer Science*, Vol. 79, pp. 1051–1059, 2016.
- [31] K. F. Jasim, K. Z. Ghafoor, and H. S. Maghdid, "Analysis of encryption algorithms proposed for data security in 4g and 5g generations," *ITM Web of Conferences*, Vol. 42. EDP Sciences, 2022, p. 01004.
- [32] A. cyber defense agency. (2021) Understanding bluetooth technology. [Online]: <https://www.cisa.gov/news-events/news/understanding-bluetooth-technology>
- [33] A. C. D. Agency. (2021) Understanding bluetooth technology. [Online]: <https://www.cisa.gov/news-events/news/understanding-bluetooth-technology#:~:text=Bluetooth%20technology%20allows%20devices%20to,is%20within%20the%20required%20distance>
- [34] A. Heinrich, M. Stute, T. Kornhuber, and M. Hollick, "Who can find my devices? security and privacy of apple's crowd-sourced bluetooth location tracking system," *arXiv preprint arXiv:2103.02282*, 2021.

- [35] U. of California. (2022) Bluetooth signals can be used to identify and track smartphones. [Online]: <https://www.sciencedaily.com/releases/2022/06/220608161407.htm>
- [36] N. Golmie, O. Rébala, and N. Chevrollier, “Bluetooth adaptive frequency hopping and scheduling,” *IEEE Military Communications Conference, 2003. MILCOM 2003.*, Vol. 2. IEEE, 2003, pp. 1138–1142.
- [37] G. Kalantar, A. Mohammadi, and S. N. Sadrieh, “Analyzing the effect of bluetooth low energy (ble) with randomized mac addresses in iot applications,” *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 27–34.
- [38] M. Kosinski. (2023) What is data privacy? [Online]: <https://www.ibm.com/topics/data-privacy>
- [39] IBM. (2023) What is data security? [Online]: <https://www.ibm.com/topics/data-security>
- [40] istarmax. How can health-tracking kids smart watches help your business succeed? [Online]: <https://istarmax.com/blog/how-can-health-tracking-kids-smart-watches-help-your-business-succeed/>
- [41] R. Mayer, “Technology, families, and privacy: Can we know too much about our loved ones?” *Journal of Consumer Policy*, Vol. 26, pp. 419–439, 12 2003.
- [42] A. Holpuch. (2022) Two women sue apple over airtag stalking. [Online]: <https://www.nytimes.com/2022/12/06/business/apple-airtag-lawsuit.html>
- [43] D. Holloway, “Surveillance capitalism and children’s data: the internet of toys and things for children,” *Media International Australia*, Vol. 170, No. 1, pp. 27–36, 2019.
- [44] K. Bryant and J. Campbell, “User behaviours associated with password security and management,” *Australasian Journal of Information Systems*, Vol. 14, No. 1, pp. 81–100, 2006.
- [45] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, “A survey on sensor-based threats and attacks to smart devices and applications,” *IEEE Communications Surveys & Tutorials*, Vol. 23, No. 2, pp. 1125–1159, 2021.
- [46] T. Kemp. (2023) The weaponization of data threats associated with data brokers. [Online]: <https://tomkemp00.medium.com/the-weaponization-of-data-threats-associated-with-data-brokers-3a27af5d8496>
- [47] T. Crepax, V. Muntés-Mulero, J. Martinez, and A. Ruiz, “Information technologies exposing children to privacy risks: domains and children-specific technical controls,” *Computer Standards & Interfaces*, Vol. 82, p. 103624, 2022.

- [48] I. Milkaite. Children’s rights to privacy and data protection around the world: Challenges in the digital realm. [Online]: <https://ejlt.org/index.php/ejlt/article/view/674/912>
- [49] X. Wang, A. K.-s. Wong, and Y. Kong, “Mobility tracking using gps, wi-fi and cell id,” *The International Conference on Information Network 2012*, 2012, pp. 171–176.
- [50] A. Moodbidri and H. Shahnasser, “Child safety wearable device,” *2017 International Conference on Information Networking (ICOIN)*, 2017, pp. 438–444.
- [51] A. Gupta and V. Harit, “Child safety tracking management system by using gps, geo-fencing android application: An analysis,” *2016 Second International Conference on Computational Intelligence Communication Technology (CICT)*, 2016, pp. 683–686.
- [52] K. Michael, A. McNamee, and M. G. Michael, “The emerging ethics of humancentric gps tracking and monitoring,” *2006 International Conference on Mobile Business*. IEEE, 2006, pp. 34–34.
- [53] B. Simpson, “Tracking children, constructing fear: Gps and the manufacture of family safety,” *Information & Communications Technology Law*, Vol. 23, No. 3, pp. 273–285, 2014.
- [54] N. C. Council, “Watchout: Analysis of smartwatches for children,” *Norwegian Consumer Council Report*, 2017.
- [55] J. Fuster, S. Solera-Cotanilla, J. Pérez, M. Vega-Barbas, R. Palacios, M. Alvarez-Campana, and G. Lopez, “Analysis of security and privacy issues in wearables for minors,” *Wireless Networks*, pp. 1–17, 2023.
- [56] M. Hron. (2019) The secret life of gps trackers. [Online]: <https://decoded.avast.io/martinhron/the-secret-life-of-gps-trackers>
- [57] M. Hannan Bin Azhar, D. Smith, and A. Cain, “Spying on kids’ smart devices: Beware of security vulnerabilities!” *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022*. Springer, 2023, pp. 123–140.
- [58] FindMyKids. (2019) Findmykids gps child tracking app: Features benefit. [Online]: <https://findmykids.org/blog/en/gps-child-tracking-appR>
- [59] C. Saatjohann, F. Ising, L. Krings, and S. Schinzel, “Stalk: Security analysis of smartwatches for kids,” *Proceedings of the 15th international conference on availability, reliability and security*, 2020, pp. 1–10.
- [60] S. Pearson and D. Allison, “Privacy compliance checking using a model-based approach,” *E-Business Applications for Product Development and Competitive Growth: Emerging Technologies*. IGI Global, 2011, pp. 199–220.

- [61] I. Reyes, P. Wijesekera, J. Reardon, A. Elazari Bar On, A. Razaghpanah, N. Vallina-Rodriguez, S. Egelman *et al.*, “Won’t somebody think of the children?” examining coppa compliance at scale,” *The 18th Privacy Enhancing Technologies Symposium (PETS 2018)*, 2018.
- [62] N. Alomar and S. Egelman, “Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps,” *Proceedings on Privacy Enhancing Technologies*, Vol. 4, No. 2022, p. 24, 2022.
- [63] K. Echenim, L. Elluri, K. P. Joshi *et al.*, “Ensuring privacy policy compliance of wearables with iot regulations,” *IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS 2023)*, 2023.
- [64] Y. Lyu, J. Gui, M. Wan, and W. G. Halfond, “An empirical study of local database usage in android applications,” *2017 IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE, 2017, pp. 444–455.
- [65] usercentricw. [Online]: <https://usercentrics.com/resources/>
- [66] O. I. Malik. (2024) The ccpa compliance checklist. [Online]: <https://securiti.ai/blog/ccpa-compliance-checklist/>
- [67] usercentricw. (2023) Compliance checklist for chinaâs pipl. [Online]: <https://securiti.ai/blog/pipl-compliance-checklist/>
- [68] O. I. Malik. (2021) Compliance checklist for south africaâs popia. [Online]: <https://securiti.ai/blog/popia-compliance-checklist/>
- [69] usercentricw. (2023) Fadp checklist. [Online]: <https://usercentrics.com/resources/fadp-checklist/>
- [70] ——. (2022) Deep learning/nlp solution for compliance subject identification. [Online]: <https://medium.com/@sridhar.palle/deep-learning-nlp-solution-for-compliance-subject-identification-30d6992aaf90>
- [71] (2023) Revolutionizing compliance with ai. [Online]: <https://www.linkedin.com/pulse/ai-revolutionizing-compliance-iprolegal/>
- [72] J. Howard and S. Ruder, “Fine-tuned language models for text classification,” *arXiv preprint arXiv:1801.06146*, Vol. 194, 2018.
- [73] N. Jiang and M.-C. de Marneffe, “Evaluating bert for natural language inference: A case study on the commitmentbank,” *Proceedings of the 2019 conference on empirical methods in natural language processing and the 9th international joint conference on natural language processing (EMNLP-IJCNLP)*, 2019, pp. 6086–6091.
- [74] A. Yates, R. Nogueira, and J. Lin, “Pretrained transformers for text ranking: Bert and beyond,” *Proceedings of the 14th ACM International Conference on web search and data mining*, 2021, pp. 1154–1156.

- [75] gareth. privacy policy. [Online]: https://gareth.com.pl/en_US/i/Privacy-policy/171
- [76] xplora. privacy policy. [Online]: <https://xplora.co.uk/pages/privacy-policy>
- [77] N. Delahanty. (2023) xplora the 1 selling smartwatch for kids. [Online]: <https://shop.myxplora.com/blogs/news/xplora-the-1-selling-smartwatch-for-kids>
- [78] (2024) gareth kids watch. [Online]: <https://watchard.com/gareth-kids-spark-4g-5903246286847-kids-watch>
- [79] P. University. Wordnet. [Online]: <https://wordnet.princeton.edu/>
- [80] B. Odonkor, S. Kaggwa, P. Uwaoma, A. Hassan, and O. Farayola, “The impact of ai on accounting practices: A review: Exploring how artificial intelligence is transforming traditional accounting methods and financial reporting,” *World Journal of Advanced Research and Reviews*, Vol. 21, pp. 172–188, 01 2024.
- [81] R. E. Hamdani, M. Mustapha, D. R. Amariles, A. Troussel, S. Meeùs, and K. Krasnashchok, “A combined rule-based and machine learning approach for automated gdpr compliance checking,” *Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law*, 2021, pp. 40–49.
- [82] O. A. Cejas, M. I. Azeem, S. Abualhaija, and L. C. Briand, “Nlp-based automated compliance checking of data processing agreements against gdpr,” *IEEE Transactions on Software Engineering*, Vol. 49, No. 9, pp. 4282–4303, 2023.
- [83] S. Chen, Y. Zhang, and Q. Yang, “Multi-task learning in natural language processing: An overview,” *ACM Computing Surveys*, 2021.

Abbreviations

| | |
|-------|---|
| ABI | Application Binary Interface |
| AITF | Active Internet Traffic Filtering |
| AWS | Amazon Web Service |
| BloSS | Blockchain Signaling System |
| CIA | Confidentiality, Integrity and Availability |
| CSIRT | Computer Security Incident Response Team |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| DNS | Domain Name System |
| DOTS | Distributed-Denial-of-Service Open Threat Signaling |
| ETH | Ether (Cryptocurrency) |
| EVM | Ethereum Virtual machine |
| IaaS | Infrastructure as a Service |
| IETF | Internet Engineering Task Force |
| IoT | Internet of Things |
| IPFS | Inter Planetary File System |
| ISP | Internet Service Provider |
| NFV | Network Function Virtualization |
| P2P | Peer to Peer |
| PoA | Proof-of-Authority |
| PoW | Proof-of-Work |
| REST | Representational State Transfer |
| RTT | Round Trip Time |
| SDN | Software-Defined Networking |
| SLA | Service Level Agreement |
| VNF | Virtualized Network Function |

List of Figures

| | | |
|-----|---|----|
| 3.1 | Checklist Schema | 16 |
| 3.2 | API development architecture diagram | 17 |
| 3.3 | UI Design | 23 |
| 3.4 | Flow Diagram Of Automated Compliance Checking System Design | 26 |
| 4.1 | Sign-In/Sign-Up Interface | 31 |
| 4.2 | Smartwatch Connectivity Interface | 32 |
| 4.3 | Area Selection Screen | 33 |
| 4.4 | Dashboard Interface | 34 |
| 4.5 | Detailed Reporting Interface | 35 |
| 4.6 | User Feedback Interface | 36 |
| 4.7 | Device Management Interface | 37 |
| 4.8 | Navigation Bar | 38 |
| 5.1 | Training and validation loss | 40 |

List of Tables

| | | |
|-----|--|----|
| 2.1 | Comparison of GPS, Cellular, Bluetooth, and Wi-Fi tracking technologies | 6 |
| 2.2 | Comparison of Children’s Privacy Regulations: CCPA, GDPR, POPIA, PIPL, nFADP | 10 |
| 3.1 | Example of checklist | 14 |
| 3.2 | Privacy Policy example | 19 |
| 3.3 | Compliance Checklist Example | 20 |
| 3.4 | Feature comparison between Xplora and Garrett smartwatches . . . | 22 |
| 4.1 | Training Arguments | 28 |
| 5.1 | Evaluation metrics for different learning rates and epochs | 40 |
| 5.2 | Evaluation Metrics for Different Augmentation Techniques | 40 |
| 5.3 | Evaluation metrics for the fine-tuned model | 41 |
| 5.4 | Metrics for checklist evaluation across various compliance regulations. | 42 |
| 5.5 | Final Metrics for checklist evaluation across various compliance regulations | 42 |
| 5.6 | Evaluation metrics for the final fine-tuned model | 42 |
| 5.7 | Example checklist questions for Garrett: Performance on Data Management and Rights | 43 |
| 5.8 | Example checklist questions for Garrett: Performance on: User Consent and Data Usage | 43 |
| 5.9 | Example checklist questions for Garrett: Performance on: Advertising and Tracking | 44 |

| | | |
|------|---|----|
| 5.10 | Example checklist questions for Xplora: Performance on: User Consent and Data Usage | 44 |
| 5.11 | Example checklist questions for Xplora: Performance on: Children's Safety | 45 |
| 5.12 | Performance of Xplora and Garrett in Different Categories | 45 |
| 5.13 | Performance of Xplora and Garrett in Different Regulations | 45 |
| 1 | The privacy policy (Xplora) | 68 |
| 2 | The privacy policy (Garrett) | 72 |
| 3 | The Whole Checklist | 75 |

Listings

| | |
|---|----|
| 4.1 Compliance Check Processing with BERT | 29 |
|---|----|

Appendix

Table 1: The privacy policy (Xplora)

| Policy ID | Watch Name | Policy |
|-----------|------------|--|
| 1 | Xplora | <p>Article 1. General Provisions</p> <p>The Xplora Watch can, together with the accompanying app and mobile telephone services subscription, collect and transmit data to XPLORA Mobile AS / XPLORA TECHNOLOGIES AS/ Xplora Technologies Ltd, such as location data. Such detailed data collection and use is critical to the successful operation of the Xplora Watch. Data collection, storage and use of data will be managed with strict privacy and security measures. Xplora App and Platform collect personal information when a user (hereinafter "you" or "Member") registers with Xplora. "Personal information" is information which identifies or can identify you or the User, such as your name, address, location data, or other data which can be reasonably linked to such information. We very much appreciate the importance of your personal information complying with all regulations and telecommunication acts, including but not limited to national Data Protection regulation as well as EU GDPR. We do our best to protect your personal information by implementing reasonable security standards and hereby inform you of the purposes and methods by which we may use your personal information of and of the actions taken to protect your privacy.</p> <p>Article 2 Data Controllers and Data Processors. Access, rectification and deletion</p> <p>For Nordic users (Norway, Sweden, Denmark, Finland and Iceland) Xplora Mobile AS, org. no. 814 499 022, is the Data Controller. For users in the other EU countries Xplora Technologies AS, Reg no: 916 752 628, is the Data Controller. For UK users, Xplora Technologies Ltd, Reg.no 10864147 is the Data Controller. You can contact us via the following email address for all the countries: policy@xplora.com You are entitled to contact one of these Data Controllers for questions related to your rights of access, rectification and deletion according to GDPR and national personal data legislation. Infomark Co Ltd, 360 Kids Guard Co., Ltd., Amazon Web Services, Zendesk Inc., and ATENDER AS are Data Processors pursuant to data processing agreements between us and these entities. All your data and personal information collected from you is subject to be processed and stored in Amazon Web Services hosted in Dublin (Ireland) and Frankfurt (Germany) on our behalf and we sometimes handle transfers from your home country to these services in Dublin (Ireland) and Frankfurt (Germany).</p> |

| | | |
|---|--------|---|
| 1 | Xplora | <p>Article 3 Categories of personal data that we collect from you and how we use it</p> <p>We may, when we provide our services to you, or in relation to our provision of services to you, collect from you and from your devices the following types of information: Service usage information, access information, cookie, IP address, mobile device identification numbers (device ID or IMEI), unauthorized or inappropriate access information, Location information stored on your device or your location information</p> <p>We may collect data from you through the following channels or methods: -through the webpage, paper form, fax, telephone, customer service board, email, promotional event application, logistics service - automatically collect from you executing or using our services -collected when you voluntarily registers for or use our service</p> <p>The legal basis for the processing of this data is for the performance of the contract of the provision of our services, entered into between you and us. In addition we may process personal data if applicable law, regulation, legal process or enforceable governmental request, obliges us to do so, or if GDPR art 6 (1) (f) is applicable, namely in cases where we have legitimate interests that are not overridden by data protection interests.</p> <p>Article 4 Information we collect based on actions on your side or if you have consented</p> <p>We may also collect following personal information in case that you use additional services or personalized services or if you participate in various events we host. In case you win an event we will process information required to provide a gift and mailing address. In case you use fee-based services we will process payment information</p> <p>We do not use your personal information for direct marketing purposes, unless a freely given, specific, informed and unambiguous consent has been obtained from you.</p> <p>Article 5 [Disclosure of Personal Information transfer to third parties]</p> <p>Your personal information will not be shared with third parties other than the ones that need this information to execute the Agreement and will not be provided to third parties or organizations beyond the scope set forth in this Privacy Policy, unless you have given consent. For the avoidance of doubt, we will not share your personal information with third parties for marketing purposes unless you give us your consent through an opt-in. However, we may disclose or use your personal information without your consent if there are any applicable law, regulation, legal process or enforceable governmental request that obliges us to do so. We may also transfer personal data to third parties if GDPR art 6 (1) (f) is applicable, namely in cases where we have legitimate interests that are not overridden by data protection interests. We may therefore pass information about the location of your Device to emergency services. Furthermore, we may provide location information or any other usage data in a non-personal, aggregate format for statistical and research purposes to third parties. Such data is not considered as personal data.</p> |
|---|--------|---|

| | | |
|---|--------|---|
| 1 | Xplora | <p>Article 6 Data retention policy</p> <p>In general, we store personal data as long as legitimate interests and/or applicable legislation, justify storage. Location data We automatically delete your location history data after 72 hours. Account data If you decide to deactivate your account by sending us an email, we keep your data for 45 days from the date of deactivation request. This is called the deactivation period and during this process your data is not accessible. Within the deactivation period you have the option to reactivate your account, unless there is a separate agreement between you and XPLORA Mobile AS or XPLORA TECHNOLOGIES AS/Xplora Technologies Ltd to begin the process of deleting your data immediately after the deactivation period has started. After the deactivation period, we will start the process of deleting your account. Deletion from our systems and backups may take up to a week. Chat messages History of chat messages are stored for, and automatically deleted, after 1 month.</p> <p>Article 7 - CHILDREN PRIVACY POLICY</p> <p>We know it's important to treat data you tell us is from children under 18 carefully. This Notice explains what we do (and don't do) when it comes to children's data.</p> <p>What Children's Data We Collect</p> <p>We don't knowingly collect data from or about children without the permission of their parent or guardian. When we do collect that data, we might do it directly, like when you sign up for a service. We might also collect it automatically if your child uses the products or services we offer. We collect the following data: - Geolocation Data â we collect data that tells us the location of your child's smart device. - Unique Identifiers â we collect device and network identifiers - basically, ways for us to tell which smart device on our network is your child's. - Customer Proprietary Network Information ("CPNI") generated by your child's use of our wireless voice communications services. - Information from your child's use of our products, services, and network (and other carriers' networks when roaming domestically or internationally) like usage of connecting carriers and Internet service providers, the Internet Protocol ("IP") address, text messages, and data use history, content interactions (e.g., how long you use an app), language settings, and other network and device analytics and Wi-Fi connection and usage data. - Device and service performance and diagnostic information â this includes reports from your child's device about signal strength, speeds, app and service performance, dropped calls, call and data failures, geolocation information, and device data. - Back-up information, including data stored in back-ups and cloud services if your child's device uploads information to XPLORA Mobile AS / XPLORA TECHNOLOGIES AS/ Xplora Technologies Ltd - Audio information, including voice commands your child provides to our app (for example, for accessibility or hands-free use). - Child's username â For joining child friendly activity-based platform Xplora Activity Platform. - Data Usage â this tells us the amount of data the hotspot uses, and IP addresses associated with websites visited. - Unique Identifiers â we collect device and network identifiers - basically, ways for us to tell which hotspot on our network is your child's.</p> <p>How We Use Children's Data</p> <p>The main reason we collect children's data is to provide the product or service that collected the data. But we may also use children's data to do things like:</p> |
|---|--------|---|

| | | |
|---|--------|--|
| 1 | Xplora | <p>- Create and administer accounts, complete transactions, payments, billing, and requests related to our products and services and third-party products and services charged to your accounts. - Check eligibility for a particular product or service. - Help stop fraudulent, malicious, deceptive, abusive, or unlawful activities. - Fix errors and ensure the quality, security, and safety of our products and services and network - Cooperate with law enforcement and protect the rights, safety, or property of our customers, XPLORE Mobile AS / XPLORE TECHNOLOGIES AS/ Xplora Technologies Ltd and others. - Comply with and enforce legal and regulatory obligations and respond to government requests. - Enforce our policies, terms and conditions, or other agreements. - Defend against or pursue claims, disputes, or litigation.</p> <p>When We Share Children's Data</p> <p>Sometimes we hire others to help us provide a product or service, and these service providers may need access to children's data. They are required to keep children's data we provide them confidential and to use it only to provide the services we requested. We may also share children's data with third parties, including the government, for legal processes or to protect life and safety where we believe that access, use, preservation, or disclosure of the data is reasonably necessary.</p> <p>Your Rights as a Parent or Guardian</p> <p>Parents and guardians have rights when it comes to their children's data: - To change their mind and withdraw consent to the collection of their child(ren)'s personal data. - To see the personal data XPLORE Mobile AS / XPLORE TECHNOLOGIES AS/ Xplora Technologies Ltd has collected about their child(ren). - To ask us to delete personal data XPLORE Mobile AS / XPLORE TECHNOLOGIES AS/ Xplora Technologies Ltd has collected about their child(ren).</p> <p>You can take any of these steps by writing email to policy@xplora.com. We may need to collect some data from you to confirm you're the parent or guardian. Important: We need to collect your child's data (as described above) to provide the relevant products or services. If you change your mind about giving consent or ask us to delete your child's data, the product or service may no longer work.</p> <p>Article 8 [Notifications on amendments to this Privacy policy]</p> <p>In the event of any material change, addition, or deletion to the privacy policy due to related laws, security technology, or due to any other matters, we will notify you of all changes with reasonable time in advance through the text message (SMS) to your mobile phone number that you provided to verify the accompanying app and through our websites, or through e-mail. Non-material changes will be notified through these websites only. *** These terms were last updated: May 2024. You will be notified if the Terms of Service in case of material changes to these Terms of Service.</p> |
|---|--------|--|

Table 2: The privacy policy (Garett)

| Policy ID | Watch Name | Policy |
|-----------|------------|---|
| 2 | Garett | <p>1. Introductory information.</p> <p>Established in the Community under the GARETT private limited company, having its registered office at: ul. Targowa 18/1413, 25-520 Kielce (referred to as: 'Operator'), acting as the owner of web page rights, which constitute to the internet store of garett.pl domain, (referred to as: 'Store'), will do its best to ensure the protection of customers privacy. Operator collect only personal data (within the meaning of the regulation form 29 August 1997, concerning the protection of personal data(i.e. The Journal of Law from 2002., No 101, item .926 further amended) (further: 'Personal data'), necessary for business activity using the store and on condition of willingly providing such details by the customer of the store. Detailed rules of processing personal details of the customer and the range of customers' acceptance for processing the details entered are specified in the following terms and conditions. Customer before placing an order of products offered in the store, accepts the processing of personal details, and can obtain full information about the scope of the very processing by the Operator.</p> <p>2. Rules of processing personal details of the customer</p> <p>Controller of the Personal Details of the store customers within the meaning of the regulation from 29 August 1997, concerning the protection of personal details (i.e. The. Journal of Law from 2002, No 101, item .926 further amended) each time is the Operator, conducting business activity under PP S.C with its registered office at: ul. Targowa 18/1413, 25-520 Kielce. The Operator collects and process the following personal details: Surname and name; Address; Company name (in case of entrepreneurs) Telephone number E-mail address NIP number (in case of entrepreneurs, in order to prepare the VAT invoice) Providing the personal details is voluntary and requires the Customers' acceptance. Operator informs that without providing personal details placing an order in the store is impossible. Operator collects and process details of people who: place the order of products provided by the Operator; contact the Operator in order to obtain the store offer information and provide personal details in the process; subscribe the Operator newsletter In case specified in point B and C, collected and processed details concern E-mail address only. In case of use of personal details for newsletter, business information will be sent to the customer via e-mail, only if customer accept the form of receiving it in such way. Customer may withdraw the acceptance for receiving newsletter from the operator via e-mail at any time. Operator collects and process the personal details in order to: complete the contract appeared due to placing the order in the store, including delivery of purchased products to the customer; answers for questions of customers and other parties; sending the subscribed correspondence and business information concerning the store offer. Operator conducts the analysis of logins and collects IP addresses of store customers for statistical purposes, maintenance and security of the domain. Operator informs that no IP address are connected to personal details of store customers.</p> |

| | | |
|---|--------|---|
| 2 | Garett | <p>In accordance to above mentioned information, a statistical data can be build (concerning store's viewing figures), which will be disclosed by the operator to third party members, including cooperating with the Operator. Operator uses network analysis systems, which may be used for creation of customer profiles. Excluding the justified reasons of marketing and customer's acceptance, the customer's profile will not be marked with name, surname or other detail which may lead to direct identification. Network analysis systems use cookie files in their processes. Personal details collected by the Operator will be processed only in the way for which it was provided in the first place, in accordance to the scope of customer's acceptance, on the basis and within the law regulation. Customer holds the right to see the content of his personal details and its correction, as well as the right to issue a written request to cease personal details processing. Correction of personal details may be performed through client contact with store service, including traditional mail and e-mails. Personal details may be shared by the operator in the necessary scope to: courier companies; operators of electronic payment systems; Subject performing, on demand of the Operator, marketing services and personalization of contact with customer.</p> <p>Customer can withdraw the acceptance for the above mentioned sharing of information and personal details at any time. Operator reserves the right to process personal details of customer, claimed in the event of performing business activity or concerning the investigation of unauthorised use of the domain. Access to personal details is available only to individuals which hold a clear written authorisation from the Operator. An authorised person dispose of individual access password to personal details. Password is not shared with others and is known to operator and authorised person only. Passwords are changed after certain period of time, on the rules specified by the operator. Lists of passwords are kept in the place available only to the Operator. Operator informs that access to personal details is also granted to authorised national authorities, within their respective ranges of competence assigned by regulations, in particular the judicial authorities (police, prosecution, courts). Operator informs that customer may only browse anonymously the content of store offered. Customer cannot anonymously, or with the use of nickname, purchase the goods of the store. In order to place an order personal details are required, specified in the following terms and conditions. Operator process the personal details in accordance with the regulation from 29 August 1997, concerning the protection of personal details (i.e. The Journal Of Law from 2000, No 101, item 926, further amended) with the use of appropriate technical and organisational means. Personal details of customers are duly secured against the access of unauthorised people, damage or deletion. Operator informs to entrust the processing of personal details to external subject only in the scope of necessary for bookkeeping and IT services, as well as in the scope of purchased goods delivery to the customer. Operator may entrust the processing of customer's personal details to subjects which execute services connected to marketing of products and services. Customer is entitled to obtain the information about subject to which it was entrusted to process his personal details, including the purpose and the scope of processing. Operator ensure the customer with direct and fixed access to the updated information specified in the point: 2.10 à 2.14, in particular, informing the customer about any changes concerning this scope. Access to information is undertaken through posting on the store's web page of an updated privacy policy and policy of cookies.</p> |
|---|--------|---|

| | | |
|---|--------|---|
| 2 | Garett | <p>4. The aim and the scope of "cookie" files use</p> <p>"Cookie" files used by the store web page enable an appropriate personalization of presented information and content adjusted to the customer, as well as measuring the user interaction within web pages. Operator uses cookie files in order to adjust and correct the way in which web page is working, as well as to measure the effectiveness of performed actions, analysis and viewing figures. Cookies enable additionally to study the customer's preferences and provide them with the most appropriate offer in accordance to these preferences. Cookie files may be used to contact the customer via mail, e-mail or telephone. Cookie files at the operator's domain may be used in particular for: measuring the activity and analysing the customers actions on the site; using the mechanism of the probe which study the customer's preferences; remembering the lack of acceptance for publishing some of the content; measuring the effectiveness (tracing of conversations) of performed actions;</p> <p>5. Types of cookie files used within the Operator's domain</p> <p>Within the Operator's domain a following types of cookie files may be used: session - which stays on the customer's appliance till the moment of leaving the site or closing the browser static - which stays on the customer's appliance throughout the period specified in the file, or till the deletion by customer.</p> <p>6. Ways of customer's resignation from the acceptance of cookie files</p> <p>Activities connected to storing and sending of cookie files are maintained by internet browsers, and stays invisible for the customer. Customer may use such settings of the browser which reject requests to store cookies in general or only to a specific types. It may be done in the browser settings. User shall know that setting off cookie files may influence the way in which the site is presented. Not finishing the settings as to cookie files means that they will be placed on the customer's final appliance, and therefore the operator may have the access to it. Usage by the customer of the store without changes in settings of the browser effect in acceptance of the above mentioned terms of cookie files use and the clearance for use by the Operator.</p> <p>7. Application and changes in the privacy policy.</p> <p>The specified privacy policy is applicable from 10 March 2015. Operator reserves the right to change the privacy policy and policy of cookies at any given moment. The consolidated text of privacy policy and policy of cookies after changes will be available on the main site of the store under bookmark "privacy policy". Information about changes will be provided to customers with two weeks advance. Any change in privacy policy and policy of cookies will be available under the "privacy policy" bookmark at the main site of the store.</p> |
|---|--------|---|

Table 3: The Whole Checklist

| User Consent and Data Usage | | | |
|-----------------------------|------------|--|--------|
| Policy ID | Regulation | Question | Answer |
| 1 | ccpa | Do you obtain explicit consent from the data subject before processing sensitive personal data or personal data from minors between the ages of 13 and 16? | 1 |
| 1 | ccpa | Do you obtain consent from a parent or legal guardian for the collection of personal data from children aged 13 or younger? | 1 |
| 1 | ccpa | Do you enable consumers to exercise their rights, such as opting out, via a banner or pop-up when they visit your site? | 1 |
| 1 | ccpa | Have you implemented a privacy notice with information about data use, consumers' rights, and user options like consent opt-out? | 1 |
| 1 | ccpa | Have you informed users about their right to opt-out of the sale or sharing of their personal data? | 1 |
| 1 | ccpa | Do you re-offer opt-in consent to consumers who have opted out, presenting the option to opt-in again after 12 months? | 1 |
| 1 | ccpa | Is there a clear and conspicuous "Do Not Sell Or Share My Personal Information" link easily accessible on your website homepage? | 0 |
| 1 | ccpa | Do you provide a "Limit The Use of My Sensitive Personal Information" link to enable opt-out? | 1 |
| 1 | ccpa | Do you ensure it is as easy to decline or change consent preferences as it is to accept? | 1 |
| 1 | ccpa | Do you obtain explicit consent from users, requiring active acceptance like ticking a box or clicking a link? | 1 |
| 1 | ccpa | Do you ensure documented consent, maintaining proof in case of an audit? | 1 |
| 1 | ccpa | Do you obtain consent in advance, ensuring no data is collected before consent is obtained? | 1 |
| 1 | ccpa | Do you obtain granular consent for individual purposes, not bundling consent with other purposes or activities? | 1 |
| 1 | ccpa | Do you make it easy to withdraw consent, with changing consent or opting out as easy as opting in? | 1 |
| 1 | ccpa | Do you ensure nonessential cookies and other tracking technologies are not triggered or loaded until valid user consent has been obtained? | 1 |
| 1 | ccpa | Do you ensure users can still access your site, app, or service even if they refuse to allow the use of nonessential cookies or other tracking technologies? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|-----------------------------------|------------------|---|---------------|
| 1 | ccpa | Do you ensure that nonconsenting users cannot be blocked entirely but can be notified about the effects on functions or services? | 1 |
| 1 | ccpa | Do you stop data collection or processing as soon as the user opts out, ensuring no data is forwarded or shared with third parties? | 1 |
| 1 | nfadp | Do you obtain and securely store user consent when required, e.g., for sensitive personal data processing? | 1 |
| 1 | pipl | Is consent for personal information processing based on the individual's willing and explicit intent with full information? | 1 |
| 1 | pipl | Do you provide a convenient method to withdraw consent? | 1 |
| 1 | pipl | Do you avoid refusing to provide a product or service to individuals based on their consent status unless necessary? | 1 |
| 1 | pipl | Do you obtain separate consent for data sharing with third parties? | 1 |
| 1 | pipl | Do you ensure users have the option to grant or withdraw consent for each purpose? | 1 |
| 1 | popia | Do you obtain users' voluntary and informed consent to store cookies on their device(s)? | 1 |
| 1 | popia | Is consent required where cookies involve the collection and processing of personal data from users (e.g., if the information can be linked to a particular individual's identity)? | 1 |
| 1 | popia | Is consent freely given with equal presentation and accessibility of 'Accept' and 'Reject' buttons? | 1 |
| 1 | popia | Is refusing consent an equally accessible option? | 1 |
| 1 | popia | Is consent easy to withdraw, with users having the option to withdraw their consent in the second layer? | 1 |
| 1 | popia | Is consent documented to provide proof in the case of an audit? | 1 |
| 1 | popia | Do you ensure that no cookies are loaded until users have given consent? | 1 |
| 1 | popia | Do you ensure that no data is collected or forwarded for declined consent for new users or updated consent preferences for existing users? | 1 |
| 1 | popia | Do you ensure that from the moment of the objection, no further data is collected or forwarded? | 1 |
| Data Management and Rights | | | |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|----------|-----------|---|--------|
| 1 | ccpa | Have you set up a system to enable the submission of Data Subject Access Requests (DSARs) allowing consumers to verify their identity and residency? | 1 |
| 1 | ccpa | Have you set up a system to enable submissions for verification requests, explaining why a request could not be verified and allowing consumers to rectify? | 1 |
| 1 | ccpa | Do you keep track of all Data Subject Access Requests (DSARs) and your business responses? | 0 |
| 1 | nfadp | Do you fulfill Data Subject Access Requests (DSARs) within the standard 45-day period or extend up to 90 days if necessary, while keeping records for 2 years? | 1 |
| 1 | nfadp | Have you created or updated internal data processing guidelines and ensured they are well communicated? | 1 |
| 1 | nfadp | Have you set up and maintained an internal registry of data processing activities? | 1 |
| 1 | nfadp | Have you implemented a process to enable efficient receipt, acknowledgment, and response to data subjects' exercising their rights, e.g., requests for copies of personal data or for correction or deletion? | 1 |
| 1 | nfadp | Is data portable in an accessible format, e.g., printout or common electronic format? | 1 |
| 1 | nfadp | Do you have a process for data breaches, including prompt notification of the FDPIC and data subjects if needed? | 0 |
| 1 | nfadp | Do you include third parties that access or process data in your data breach process? | 1 |
| 1 | ccpa | Have you informed users about their right to know what personal data is collected and how it is used or shared? | 1 |
| 1 | ccpa | Have you informed users about their right to delete personal data that has been collected about them, with exceptions? | 1 |
| 1 | ccpa | Have you informed users about their right to data portability, providing a copy of personal data in a portable and readily usable format? | 1 |
| 1 | ccpa | Have you informed users about their right to non-discrimination for exercising privacy rights? | 0 |
| 1 | gdpr | Do you inform users about their right of access to be informed if personal data is processed, what data, and receive access to it? | 1 |
| 1 | gdpr | Do you inform users about their right to rectification, timely updates, or corrections to inaccuracies in personal data collected? | 1 |

Continued on next page

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|---|------------------|--|---------------|
| 1 | gdpr | Do you inform users about their right to erasure, timely deletion of personal data that has been collected, and notification from the processor when complete? | 1 |
| 1 | gdpr | Do you inform users about their right to restriction of processing, the processor must stop processing personal data temporarily or permanently? | 1 |
| 1 | gdpr | Do you inform users about their right to data portability, providing a copy of personal data in a portable and readily usable format? | 1 |
| 1 | gdpr | Do you inform users about their right to object to the processing of personal data, including sharing, sale, or profiling? | 1 |
| 1 | gdpr | Do you inform users about their right to know about automated decision-making and the likely outcomes of using it, including profiling? | 1 |
| 1 | gdpr | Do you inform users about their right to opt out of automated decision-making technology with regards to personal data, including profiling? | 1 |
| 1 | gdpr | Do you inform users about their right to non-discrimination for exercising privacy rights? | 1 |
| 1 | gdpr | Are you able to provide users with the data specified by the GDPR's 'Rights of the data subject' in a timely fashion in the event of a data subject access request (DSAR)? | 1 |
| 1 | pipl | Do you assess and obtain consent from parents or guardians for processing personal information of minors under 14? | 0 |
| 1 | pipl | Do you ensure individuals have rights such as being informed, decision, restriction and objection, access and copy, rectification, deletion, data portability, and refusal of automated decision-making? | 1 |
| 1 | pipl | Do you establish mechanisms to handle rights requests from individuals and provide explanations for any rejections? | 1 |
| Privacy Policies and Practices - Data Handling | | | |
| 1 | ccpa | Have you created a comprehensive Privacy Policy informing consumers at or before the point of data collection about how data is collected, retained, and used? | 1 |
| 1 | ccpa | Does your Privacy Policy inform consumers about the categories of personal data collected and the purposes for which it is collected? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|------------------------|-----------|--|--------|
| 1 | ccpa | Does your Privacy Policy disclose whether collected data is sold to or shared with third parties and identify those third parties? | 1 |
| 1 | ccpa | Does your Privacy Policy inform website visitors of their privacy rights and how to exercise them? | 1 |
| 1 | ccpa | Is your Privacy Policy clear, easy to understand, and available in the languages in which your business provides information in California? | 1 |
| 1 | ccpa | Do you review and update your Privacy Policy every 12 months, reflecting any changes in operations or law? | 1 |
| 1 | ccpa | Do you ensure the effective date of your Privacy Policy is updated every 12 months, even if no other changes are made? | 1 |
| 1 | ccpa | Do you provide at least two contact options, such as a toll-free phone number, web form, or email, for consumers to reach you? | 1 |
| 1 | nfadp | Do you review and update your Privacy Policy every 12 months? | 1 |
| 1 | nfadp | Have you created a comprehensive Privacy Policy? | 1 |
| 1 | nfadp | Does your Privacy Policy detail how data is collected? | 1 |
| 1 | nfadp | Does your Privacy Policy state how long collected data is retained? | 1 |
| 1 | nfadp | Does your Privacy Policy specify the categories of personal data collected? | 1 |
| 1 | nfadp | Does your Privacy Policy describe the purposes for which data is collected? | 1 |
| 1 | nfadp | Does your Privacy Policy indicate whether data collected is sold to or shared with third parties? | 1 |
| 1 | nfadp | Does your Privacy Policy name the third parties with which data is shared? | 1 |
| 1 | nfadp | Do you inform website visitors of their privacy rights and how to exercise them? | 1 |
| 1 | nfadp | Is your Privacy Policy clear and easy to understand? | 1 |
| 1 | nfadp | Is your Privacy Policy available in the languages in which your business provides information in California? | 1 |
| 1 | nfadp | Have you implemented a privacy notice with information about data use, consumers' rights, and user options, like consent opt-out? | 1 |
| 1 | nfadp | Have you enabled consumers to exercise rights, like opting out, via a banner or pop-up when users visit your site, e.g., with a Consent Management Platform? | 1 |
| 1 | nfadp | Have you ensured data subjects are informed prior to data collection even if consent is not required? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|------------------------|-----------|--|--------|
| 1 | nfadp | Does your notification include the identity of the data controller, whether the company or a third party? | 1 |
| 1 | nfadp | Does your notification provide contact details for the data controller? | 1 |
| 1 | nfadp | Does your notification include the identity of the data recipient and any other parties involved with the data file? | 1 |
| 1 | nfadp | Does your notification specify the recipient country if the data will be transferred cross-border? | 1 |
| 1 | nfadp | Does your notification detail the purpose(s) of data collection and use? | 1 |
| 1 | nfadp | Does your notification explain what categories of data are collected, if relevant? | 1 |
| 1 | nfadp | Does your notification describe the means of data collection, if relevant? | 1 |
| 1 | nfadp | Does your notification specify the legal basis for processing, if needed? | 1 |
| 1 | nfadp | Does your notification inform users of their rights regarding their personal data under the FADP, including the right to refuse or withdraw consent? | 1 |
| 1 | nfadp | Have you created privacy statements, like a privacy policy page on the website, or updated existing ones? | 1 |
| 1 | nfadp | Are your privacy statements customized for your business, users, processing purposes, and the data you process? | 1 |
| 1 | nfadp | Does your consent management platform enable customizing and populating your privacy policy, as well as keeping it updated? | 1 |
| 1 | nfadp | Does your notification information include with which countries personal data is shared? | 1 |
| 1 | nfadp | Do you make it clear if there is no adequacy agreement with those countries and get explicit consent for data sharing? | 0 |
| 1 | gdpr | Do you inform consumers at or before the point of data collection how data is collected? | 1 |
| 1 | gdpr | Do you inform consumers at or before the point of data collection how long collected data is retained? | 1 |
| 1 | gdpr | Do you inform consumers at or before the point of data collection the categories of personal data collected? | 1 |
| 1 | gdpr | Do you inform consumers at or before the point of data collection the purposes for which data is collected? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|------------------------|-----------|--|--------|
| 1 | gdpr | Do you inform consumers at or before the point of data collection whether data collected is sold to or shared with third parties? | 1 |
| 1 | gdpr | Do you inform consumers at or before the point of data collection the third parties with which data is sold or shared? | 1 |
| 1 | gdpr | Do you inform website visitors of their privacy rights and how to exercise them? | 1 |
| 1 | gdpr | Is the Privacy Policy and cookie banner clear and easy to understand? | 1 |
| 1 | gdpr | Do you have a valid legal basis for data processing, and is consent one legal basis? | 1 |
| 1 | gdpr | Do you provide informed consent detailing who, what, why, and how long data is processed? | 1 |
| 1 | gdpr | Do you review your operations and potential changes in the law every 12 months? | 1 |
| 1 | gdpr | Do you update your Privacy Policy information and its effective date every 12 months? | 1 |
| 1 | gdpr | Do you ensure the information that users must be notified about is clear, comprehensive, and up to date? | 1 |
| 1 | gdpr | Do you list all the categories of personal information that your business has sold in the past 12 months? | 1 |
| 1 | gdpr | If the consumer has opted out, do you present the option to opt-in again after 12 months? | 1 |
| 1 | pipl | Is your privacy notice clear and easy to understand, and does it include the required information such as handler's contact, purpose, methods, categories, and retention period of personal information? | 1 |
| 1 | pipl | Do you notify individuals about any changes to the privacy notice? | 1 |
| 1 | pipl | Do you notify individuals about third-party data recipients, their contact information, processing purpose and method, and personal information categories? | 1 |
| 1 | pipl | Do you avoid providing personal information stored in China to foreign authorities without Chinese authorities' approval? | 1 |
| 1 | pipl | Do you establish specialized processing rules for minors' data? | 0 |
| 1 | pipl | Do you appoint personal information protection officers and disclose their contact information? | 0 |
| 1 | pipl | Do you adopt technical measures such as encryption and de-identification to ensure the security of personal information processing? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|---------------------------------|-----------|--|--------|
| 1 | pipl | Do you retain personal information for the shortest period necessary to achieve the processing purpose? | 1 |
| 1 | pipl | Do you conduct regular education and training on personal information security for employees? | 1 |
| 1 | pipl | Do you sign data processing agreements with vendors and supervise their processing activities? | 1 |
| 1 | pipl | Do you ensure vendors take necessary measures to safeguard personal information security and assist in fulfilling PIPL obligations? | 1 |
| 1 | pipl | Do you formulate and implement security incident response plans and notify competent authorities and individuals about any data breaches? | 1 |
| 1 | popia | Do you include the above information in your Privacy Policy? | 1 |
| 1 | popia | Do you explain in the first layer of the privacy banner what your cookies or other web technologies are doing and why? | 1 |
| Children's Safety | | | |
| 1 | ccpa | Have you obtained consent from a parent or guardian before collecting personal data from children? | 1 |
| 1 | ccpa | Do you obtain explicit consent from the data subject before processing sensitive personal data or personal data from minors between the ages of 13 and 16? | 1 |
| 1 | ccpa | Do you obtain consent from a parent or legal guardian for the collection of personal data from children aged 13 or younger? | 1 |
| 1 | ccpa | Do you ensure the effective date of your Privacy Policy is updated every 12 months, even if no other changes are made? | 1 |
| 1 | ccpa | Do you re-offer opt-in consent to consumers who have opted out, presenting the option to opt-in again after 12 months? | 1 |
| 1 | pipl | Do you assess and obtain consent from parents or guardians for processing personal information of minors under 14? | 0 |
| 1 | pipl | Do you establish specialized processing rules for minors' data? | 0 |
| Advertising and Tracking | | | |
| 1 | ccpa | Do you have a clear and conspicuous "Do Not Sell Or Share My Personal Information" link easily accessible on your website homepage? | 0 |
| 1 | ccpa | Do you provide a "Limit The Use of My Sensitive Personal Information" link to enable opt-out? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|----------|-----------|--|--------|
| 1 | gdpr | Have you enabled geolocation features to customize language displayed for users in different regions? | 1 |
| 1 | gdpr | Do you ensure documented consent, maintaining proof in case of an audit? | 1 |
| 1 | gdpr | Do you obtain consent in advance, ensuring no data is collected before consent is obtained? | 1 |
| 1 | gdpr | Do you obtain granular consent for individual purposes, not bundling consent with other purposes or activities? | 1 |
| 1 | gdpr | Do you make it easy to withdraw consent, with changing consent or opting out as easy as opting in? | 1 |
| 1 | gdpr | Do you ensure nonessential cookies and other tracking technologies are not triggered or loaded until valid user consent has been obtained? | 1 |
| 1 | gdpr | Do you ensure users can still access your site, app, or service even if they refuse to allow the use of nonessential cookies or other tracking technologies? | 1 |
| 1 | gdpr | Do you ensure that nonconsenting users cannot be blocked entirely but can be notified about the effects on functions or services? | 1 |
| 1 | gdpr | Do you stop data collection or processing as soon as the user opts out, ensuring no data is forwarded or shared with third parties? | 1 |
| 1 | gdpr | Do you provide informed consent detailing who, what, why, and how long data is processed? | 1 |
| 1 | popia | Do you inform users that you use cookies or other tracking technologies at or before the point you start collecting data? | 1 |
| 1 | popia | Do you inform users about the purpose of each cookie or web technology separately to ensure specific and granular consent for each cookie objective? | 0 |
| 1 | popia | Do you ensure that no cookies are loaded until users have given consent? | 1 |
| 1 | popia | Do you ensure that no data is collected or forwarded for declined consent for new users or updated consent preferences for existing users? | 1 |
| 1 | popia | Do you ensure that from the moment of the objection, no further data is collected or forwarded? | 1 |
| 2 | ccpa | Have you obtained consent from a parent or guardian before collecting personal data from children? | 1 |
| 2 | ccpa | Do you obtain explicit consent from the data subject before processing sensitive personal data or personal data from minors between the ages of 13 and 16? | 0 |

Continued on next page

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|------------------------|-----------|---|--------|
| 2 | ccpa | Do you obtain consent from a parent or legal guardian for the collection of personal data from children aged 13 or younger? | 0 |
| 2 | ccpa | Do you re-offer opt-in consent to consumers who have opted out, presenting the option to opt-in again after 12 months? | 0 |
| 2 | nfadp | Have you enabled consumers to exercise rights, like opting out, via a banner or pop-up when users visit your site, e.g., with a Consent Management Platform? | 0 |
| 2 | nfadp | Do you obtain and securely store user consent when required, e.g., for sensitive personal data processing? | 1 |
| 2 | gdpr | Do you obtain explicit consent from users, requiring active acceptance like ticking a box or clicking a link? | 1 |
| 2 | gdpr | Do you provide informed consent detailing who, what, why, and how long data is processed? | 1 |
| 2 | gdpr | Do you ensure documented consent, maintaining proof in case of an audit? | 1 |
| 2 | gdpr | Do you obtain consent in advance, ensuring no data is collected before consent is obtained? | 0 |
| 2 | gdpr | Do you obtain granular consent for individual purposes, not bundling consent with other purposes or activities? | 0 |
| 2 | gdpr | Do you make it easy to withdraw consent, with changing consent or opting out as easy as opting in? | 1 |
| 2 | gdpr | Do you ensure nonessential cookies and other tracking technologies are not triggered or loaded until valid user consent has been obtained? | 0 |
| 2 | gdpr | Do you ensure users can still access your site, app, or service even if they refuse to allow the use of nonessential cookies or other tracking technologies? | 0 |
| 2 | gdpr | Do you ensure that nonconsenting users cannot be blocked entirely but can be notified about the effects on functions or services? | 0 |
| 2 | popia | Do you ensure users have the option to grant or withdraw consent for each purpose? | 0 |
| 2 | popia | Do you obtain users' voluntary and informed consent to store cookies on their device(s)? | 1 |
| 2 | popia | Is consent required where cookies involve the collection and processing of personal data from users (e.g., if the information can be linked to a particular individual's identity)? | 1 |
| 2 | popia | Is consent freely given with equal presentation and accessibility of 'Accept' and 'Reject' buttons? | 1 |
| 2 | popia | Is refusing consent an equally accessible option? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|-----------------------------------|-----------|---|--------|
| 2 | popia | Is consent easy to withdraw, with users having the option to withdraw their consent in the second layer? | 1 |
| 2 | popia | Is consent documented to provide proof in the case of an audit? | 1 |
| 2 | popia | Do you ensure that no cookies are loaded until users have given consent? | 0 |
| 2 | pipl | Is consent for personal information processing based on the individual's willing and explicit intent with full information? | 1 |
| 2 | pipl | Do you provide a convenient method to withdraw consent? | 0 |
| 2 | pipl | Do you obtain separate consent for data sharing with third parties? | 0 |
| 2 | pipl | Do you obtain separate consent for processing sensitive personal information if no other lawful basis can be relied on? | 0 |
| 2 | pipl | Do you notify individuals about data importer's details, processing purpose, methods, and categories, and obtain separate consent for cross-border data transfer? | 0 |
| Data Management and Rights | | | |
| 2 | ccpa | Do you provide at least two contact options, such as a toll-free phone number, web form, or email, for consumers to reach you? | 1 |
| 2 | ccpa | Have you set up a system to enable the submission of Data Subject Access Requests (DSARs) allowing consumers to verify their identity and residency? | 1 |
| 2 | ccpa | Have you set up a system to enable submissions for verification requests, explaining why a request could not be verified and allowing consumers to rectify? | 1 |
| 2 | ccpa | Do you keep track of all Data Subject Access Requests (DSARs) and your business responses? | 0 |
| 2 | ccpa | Do you fulfill Data Subject Access Requests (DSARs) within the standard 45-day period or extend up to 90 days if necessary, while keeping records for 2 years? | 1 |
| 2 | nfadp | Have you implemented a process to enable efficient receipt, acknowledgment, and response to data subjects' exercising their rights, e.g., requests for copies of personal data or for correction or deletion? | 1 |
| 2 | nfadp | Is data portable in an accessible format, e.g., printout or common electronic format? | 1 |
| 2 | nfadp | Have you implemented a data protection impact assessment, especially if the organization extensively processes sensitive data? | 0 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|---|------------------|--|---------------|
| 2 | nfadp | Do you have a process for data breaches, including prompt notification of the FDPIC and data subjects if needed? | 0 |
| 2 | nfadp | Do you include third parties that access or process data in your data breach process? | 1 |
| 2 | nfadp | Have you set up and maintained an internal registry of data processing activities? | 1 |
| 2 | nfadp | Do you review and update your Privacy Policy every 12 months? | 0 |
| 2 | nfadp | Have you appointed a data protection officer who liaises with users and the FDPIC, and administers policies and processes? | 0 |
| 2 | nfadp | Do you consult with qualified legal counsel regarding your organization's responsibilities under the FADP and how to fulfill them? | 1 |
| 2 | nfadp | Do you review your operations and potential changes in the law every 12 months? | 0 |
| 2 | gdpr | Do you ensure documented consent, maintaining proof in case of an audit? | 1 |
| 2 | gdpr | Are you able to verify users' consent for all data collected and the processing purposes in the event of an audit by data protection authorities? | 0 |
| 2 | gdpr | Are you able to provide users with the data specified by the GDPR's 'Rights of the data subject' in a timely fashion in the event of a data subject access request (DSAR)? | 1 |
| 2 | popia | Do you document and store consent received from users to comply with documentation obligations and ensure verification in case of complaint or audit? | 0 |
| 2 | popia | Do you ensure that from the moment of the objection, no further data is collected or forwarded? | 0 |
| 2 | popia | Do you ensure that no data is collected or forwarded for declined consent for new users or updated consent preferences for existing users? | 1 |
| 2 | pipl | Do you ensure individuals have rights such as being informed, decision, restriction and objection, access and copy, rectification, deletion, data portability, and refusal of automated decision-making? | 1 |
| 2 | pipl | Do you establish mechanisms to handle rights requests from individuals and provide explanations for any rejections? | 1 |
| Privacy Policies and Practices - Data Handling | | | |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|------------------------|-----------|--|--------|
| 2 | ccpa | Have you created a comprehensive Privacy Policy informing consumers at or before the point of data collection about how data is collected, retained, and used? | 1 |
| 2 | ccpa | Does your Privacy Policy inform consumers about the categories of personal data collected and the purposes for which it is collected? | 1 |
| 2 | ccpa | Does your Privacy Policy disclose whether collected data is sold to or shared with third parties and identify those third parties? | 1 |
| 2 | ccpa | Do you review and update your Privacy Policy every 12 months, reflecting any changes in operations or law? | 0 |
| 2 | ccpa | Do you ensure the effective date of your Privacy Policy is updated every 12 months, even if no other changes are made? | 0 |
| 2 | nfadp | Have you created a comprehensive Privacy Policy? | 1 |
| 2 | nfadp | Does your Privacy Policy detail how data is collected? | 1 |
| 2 | nfadp | Does your Privacy Policy state how long collected data is retained? | 1 |
| 2 | nfadp | Does your Privacy Policy specify the categories of personal data collected? | 1 |
| 2 | nfadp | Does your Privacy Policy describe the purposes for which data is collected? | 1 |
| 2 | nfadp | Does your Privacy Policy indicate whether data collected is sold to or shared with third parties? | 1 |
| 2 | nfadp | Does your Privacy Policy name the third parties with which data is shared? | 1 |
| 2 | nfadp | Do you inform website visitors of their privacy rights and how to exercise them? | 1 |
| 2 | nfadp | Is your Privacy Policy clear and easy to understand? | 1 |
| 2 | nfadp | Is your Privacy Policy available in the languages in which your business provides information in California? | 1 |
| 2 | nfadp | Have you implemented a privacy notice with information about data use, consumers' rights, and user options, like consent opt-out? | 1 |
| 2 | nfadp | Have you ensured data subjects are informed prior to data collection even if consent is not required? | 1 |
| 2 | nfadp | Does your notification include the identity of the data controller, whether the company or a third party? | 1 |
| 2 | nfadp | Does your notification provide contact details for the data controller? | 1 |
| 2 | nfadp | Does your notification detail the purpose(s) of data collection and use? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|-----------------|------------------|--|---------------|
| 2 | nfadp | Does your notification explain what categories of data are collected, if relevant? | 1 |
| 2 | nfadp | Does your notification specify the legal basis for processing, if needed? | 1 |
| 2 | nfadp | Does your notification inform users of their rights regarding their personal data under the FADP, including the right to refuse or withdraw consent? | 1 |
| 2 | nfadp | Have you created privacy statements, like a privacy policy page on the website, or updated existing ones? | 1 |
| 2 | nfadp | Are your privacy statements customized for your business, users, processing purposes, and the data you process? | 1 |
| 2 | nfadp | Does your consent management platform enable customizing and populating your privacy policy, as well as keeping it updated? | 0 |
| 2 | nfadp | Does your notification information include with which countries personal data is shared? | 1 |
| 2 | nfadp | Do you make it clear if there is no adequacy agreement with those countries and get explicit consent for data sharing? | 0 |
| 2 | nfadp | Do you maintain data only for as long as necessary under the stated notification and for the stated purpose of processing? | 1 |
| 2 | nfadp | Do you delete or anonymize data as soon as it is no longer required for that purpose? | 1 |
| 2 | gdpr | Do you inform consumers at or before the point of data collection the third parties with which data is sold or shared? | 1 |
| 2 | gdpr | Do you inform consumers at or before the point of data collection how data is collected? | 1 |
| 2 | gdpr | Do you inform consumers at or before the point of data collection the purposes for which data is collected? | 1 |
| 2 | gdpr | Do you inform consumers at or before the point of data collection whether data collected is sold to or shared with third parties? | 1 |
| 2 | gdpr | Do you inform website visitors of their privacy rights and how to exercise them? | 1 |
| 2 | gdpr | Is the Privacy Policy and cookie banner clear and easy to understand? | 1 |
| 2 | gdpr | Have you implemented a privacy notice with information about data use, consumers' rights, and user options, like consent opt-out? | 1 |

Continued on next page

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|------------------------|-----------|--|--------|
| 2 | gdpr | Do you ensure consumers can access your Privacy Policy, which includes the above information, in a clear and easy-to-understand format? | 1 |
| 2 | gdpr | Do you have a valid legal basis for data processing, and is consent one legal basis? | 1 |
| 2 | gdpr | Do you ensure the information that users must be notified about is clear, comprehensive, and up to date? | 1 |
| 2 | popia | Does your Privacy Policy ensure it is easy to find, read, and understand for the average user? | 1 |
| 2 | popia | Does your Privacy Policy inform about who has access to personal data collected (e.g., from cookies)? | 1 |
| 2 | popia | Have you implemented the information and consent preferences about data processing in a Privacy Banner when users visit your site? | 1 |
| 2 | popia | Do you inform users about the specific purpose of the processing? | 1 |
| 2 | popia | Do you inform users about the type and duration of the processing? | 1 |
| 2 | popia | Do you inform users about the identity of the responsible party and their contact information? | 1 |
| 2 | popia | Do you inform users about the shared use of data by the responsible party and the purpose? | 1 |
| 2 | popia | Do you inform users about the responsibilities of the agents that will carry out the processing? | 1 |
| 2 | popia | Do you inform users about the data subject's rights with explicit mention of the rights listed in Section 5 of POPIA? | 1 |
| 2 | popia | Do you include the above information in your Privacy Policy? | 1 |
| 2 | pipl | Is your privacy notice clear and easy to understand, and does it include the required information such as handler's contact, purpose, methods, categories, and retention period of personal information? | 1 |
| 2 | pipl | Do you notify individuals about any changes to the privacy notice? | 1 |
| 2 | pipl | Do you notify individuals about third-party data recipients, their contact information, processing purpose and method, and personal information categories? | 1 |
| 2 | pipl | Do you have a lawful basis for personal information processing such as consent, contract performance, statutory responsibility, public health emergency, public interest purposes, or legally disclosed information? | 1 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|--------------------------|------------------|---|---------------|
| 2 | pipl | Do you establish specialized processing rules for minors' data? | 1 |
| 2 | pipl | Do you avoid refusing to provide a product or service to individuals based on their consent status unless necessary? | 1 |
| 2 | pipl | Do you ensure transparency, fairness, and justice in automated decision-making? | 1 |
| 2 | pipl | Do you provide options to opt-out of automated decision-making? | 1 |
| 2 | pipl | Do you use CCTV and facial recognition technology only for safeguarding public security and with clear signs? | 1 |
| 2 | pipl | Are you processing any sensitive personal information in China such as biometric characteristics, religious beliefs, medical health, financial accounts, or information of minors under 14? | 1 |
| 2 | pipl | Do you have a specific purpose and sufficient necessity for processing sensitive personal information, and take strict protection measures? | 0 |
| 2 | pipl | Do you adopt technical measures such as encryption and de-identification to ensure the security of personal information processing? | 1 |
| 2 | pipl | Do you retain personal information for the shortest period necessary to achieve the processing purpose? | 1 |
| 2 | pipl | Do you sign data processing agreements with vendors and supervise their processing activities? | 1 |
| 2 | pipl | Do you ensure vendors take necessary measures to safeguard personal information security and assist in fulfilling PIPL obligations? | 1 |
| 2 | pipl | Do you formulate and implement security incident response plans and notify competent authorities and individuals about any data breaches? | 1 |
| Children's Safety | | | |
| 2 | ccpa | Have you obtained consent from a parent or guardian before collecting personal data from children? | 1 |
| 2 | ccpa | Do you obtain explicit consent from the data subject before processing sensitive personal data or personal data from minors between the ages of 13 and 16? | 0 |
| 2 | ccpa | Do you obtain consent from a parent or legal guardian for the collection of personal data from children aged 13 or younger? | 0 |
| 2 | pipl | Do you assess and obtain consent from parents or guardians for processing personal information of minors under 14? | 0 |
| Continued on next page | | | |

Table 3 – continued from previous page

| Category | Policy ID | Question | Answer |
|---------------------------------|-----------|--|--------|
| 2 | pipl | Do you establish specialized processing rules for minors' data? | 1 |
| Advertising and Tracking | | | |
| 2 | nfadp | Have you enabled consumers to exercise rights, like opting out, via a banner or pop-up when users visit your site, e.g., with a Consent Management Platform? | 0 |
| 2 | gdpr | Do you ensure nonessential cookies and other tracking technologies are not triggered or loaded until valid user consent has been obtained? | 0 |
| 2 | gdpr | Do you ensure users can still access your site, app, or service even if they refuse to allow the use of nonessential cookies or other tracking technologies? | 0 |
| 2 | gdpr | Do you ensure that nonconsenting users cannot be blocked entirely but can be notified about the effects on functions or services? | 0 |
| 2 | gdpr | Do you make it easy to withdraw consent, with changing consent or opting out as easy as opting in? | 1 |
| 2 | popia | Do you ensure users have the option to grant or withdraw consent for each purpose? | 0 |
| 2 | popia | Do you obtain users' voluntary and informed consent to store cookies on their device(s)? | 1 |
| 2 | popia | Do you ensure that no cookies are loaded until users have given consent? | 0 |