UNIVERSIDADE
FEDERAL RURAL
DE PERNAMBUCO

Maria Eduarda Rebelo Di Carlli

Towards a Quality Audit Process for Children's Privacy Policies

Recife

2023

Maria Eduarda Rebelo Di Carlli

Towards a Quality Audit Process for Children's Privacy Policies

Master's Thesis presented to the members of M.Sc in Computer Science from Federal Rural University of Pernambuco as partial requirement to achieve title of M.Sc in Computer Science.

Federal Rural University of Pernambuco (UFRPE)

Department of Computing (DC)

M.Sc in Computer Science

Supervisor: Prof. Fernando Antônio Aires Lins, PhD

Co-supervisor: Prof. George Augusto Valença Santos, PhD

Recife

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

D536t Di Carlli, Maria Eduarda Rebelo
Towards a Quality Audit Process for Children’s Privacy Policies / Maria Eduarda Rebelo Di Carlli. - 2023.
125 f.

Orientador: Fernando Antonio Aires Lins.
Coorientador: George Augusto Valenca Santos.
Inclui referências, apêndice(s) e anexo(s).

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação em Informática Aplicada, Recife, 2023.

1. Privacy. 2. Privacy Policy. 3. Data Protection. 4. Children's Privacy. 5. Wearables. I. Lins, Fernando Antonio Aires, orient. II. Santos, George Augusto Valenca, coorient. III. Título

CDD 004

“And once the storm is over you won’t remember how you made it through, how you managed to survive. You won’t even be sure, in fact, whether the storm is really over. But one thing is certain – when you come out of the storm, you won’t be the same person who walked in. That’s what this storm’s all about.”

(Haruki Murakami)

Acknowledgements

To my dear parents Giovanni and Patricia, and brother Pedro, for the undying support and understanding throughout my entire academic journey. Sacrifices were made to navigate the ups and downs of the past two years, so thank you for understanding and supporting me for the duration of it.

To my supervisors Fernando Aires e George Valença, Ph.D., for the unfaltering belief that I could cross the finish line by offering my absolute best. Thank you for understanding, for supporting, and for the reassuring faith in the work I was doing. This is a product of our combined efforts and I will be eternally grateful.

To my friend Nikoo Saber, Ph.D., for being one of the reasons I was able to get this far. Your utmost support has made and will continue to make a positive difference in my life. Thank you for being a mentor, a teacher, a listening ear and a friend. My gratitude is endless and everlasting.

To my friend Victor Alexandre, for being a crucial support system that helped keep me afloat while I trod these turbulent waters. Thank you for being an spectacular human being and friend, and a voice of reason when needed.

To my friend Ariany Ferreira, my partner in crime for years in this so-called life — academic or otherwise. Thank you for being there through the good and the bad, the hardships and celebrations, and everything else in between.

To all the professors and staff members of Departament of Statistics and Informatics (DEINFO) at Universidade Federal Rural de Pernambuco, for the ongoing support provided to students throughout the years.

And to every person who, directly or indirectly, contributed to this work and my academic journey: I am and will always be grateful.

Abstract

Concerns around the protection of children's personal information has grown exponentially over the years as this audience continues to be introduced to technology at an early age. The adoption of wearables to increase physical activity levels among children raises questions from both parents and guardians, as well as researchers, as to the kind of data being processed by these devices, how each company handles such sensitive data, and most importantly, whether or not those practices are denoted in their privacy policy. With the implementation of laws centred on data privacy and protection over the past decade, additional requirements in children-related laws, such as the Children's Online Privacy Protection Act (COPPA), serve as an added layer of holding companies accountable for not providing clear and straightforward privacy-related information to the user. This research investigates how privacy policies are provided to the user and what kind of information is made available to parents and guardians by the companies that offer products targeted at children. We propose an audit process that evaluates privacy policies for products targeted at children with goal of assessing the quality of the information provided to the user and whether the policies meet the requirements from laws and regulations to provide compliance-driven directives. The results showcase that there is a common practice of not allowing these policies to be easily accessible by the user on the companies' websites and that they generally fail to provide crucial details on the type of security practices involved in the data handling process. Lastly, we discuss the impact of the raised concerns in the delivery of these policies to parents and guardians and how the proposed audit can assist companies to deliver privacy policies with quality and transparency in a compliance-driven manner.

Keywords: Privacy, Privacy Policy, Data Protection, Children's Privacy, Quality Criteria, Audit, Fitness Trackers, Wearables

Contents

List of Figures

List of Tables

1 Introduction

1.1 Context and Problem

Over the past decade, the use of ubiquitous technologies has been rapidly spreading among different spheres of people's lives (FIETKIEWICZ; ILHAN, 2020). The estimated market size for smart wearables – which includes smartwatches, smart clothing, fitness trackers, medical devices – is around $70.5 billion in 2023, with projections to reach $171.66 billion by 2028 according to a report by Mordor Intelligence[1]. A substantial growth in interest for currently available fitness trackers has been observed in children and adolescents, while positive results regarding the measurement of their physical activity levels directly impacts the increasing adherence among those groups (MACKINTOSH et al., 2019). Security and privacy related discussions have also grown, both in the media and in academia, as the protection of minors' personal data takes centre stage. When fitness and activity trackers are concerned, given the sensitive nature of the data in question, studies surrounding the current market situation and analysing security and privacy of these devices is pertinent (FúSTER et al., 2023)

Although there is an observed increase in purchase of wearables from lesser-know brands, companies like Garmin, Fitbit (acquired by Google in 2021), Apple, and Xiaomi continue to dominate the industry of smartwatches and fitness trackers. It is understood that users gravitating towards these influential tech companies is a direct result of the latter exercising different types of powers over these users, enabled by elements such as reputation and technical orchestration to evoke a sense of trust and convenience (REBELO; VALENçA; LINS, 2021), despite some such companies having notoriously failed to comply with regulations and been involved in data breach reports over the past few years.

The combination of these factors has urged legal entities to reinforce punishments and surveillance regarding compliance with privacy requirements, especially concerning children. The Children's Online Privacy Protection Rule (COPPA), for the past five years, has served as a legal enabler for the Federal Trade Commission (FTC) to hold companies accountable for potential mishandling of minors' data without parents' permission or selling children's personal information. In 2022, Kurbo, a weight management service for children and teens offered by WW International, was fined by the FTC with a $1.5M civil penalty for collecting data such as weight, food intake, and activity without parental consent. Additionally, all personal information collected from kids under 13 without parental permission had to be deleted and any algorithms that were used to illegally collect information to be destroyed [2].

[1] Smart Wearables Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028) - Mordor Intelligence <https://www.mordorintelligence.com/industry-reports/smart-wearables-market>

[2] Kurbo by WW charged with collecting kids' personal info without parents' permis-

In 2022, the Children's Advertising Review Unit (CARU) reported that TickTalk Tech, the company behind TickTalk 4, a smartwatch for children, was in violation of COPPA for not providing clear and upfront information to parents and guardians in their privacy policies, as well as highlighting that the company does not display their privacy policy prominently to the user. Among the corrective actions, CARU determined a correction of all TickTalk's privacy policy instances (i.e. website/app) to provide *"complete, accurate, consistent, and non-confusing statement of its information collection, use, and disclosure practices regarding children's personal information"* and include clear notice to parents of *"collection, use and disclosure practices, and prior to parents' completion of the registration process, provide a clear, prominent, and unavoidable means to obtain verifiable consent"*[3].

Despite legal actions taken by regulators to hold companies accountable for mishandling data or not providing clear information, significant gaps are still observed in the privacy policies they provide for their services, suggesting that compliance in its entirety remains an afterthought and not considered as part of a structured process that conducts an evaluation of the content of these privacy policies prior to reaching the user.

1.2 Motivation

This research is driven by the question of how privacy policies are provided to the user and what kind of information is made available to parents and guardians by the companies that offer products targeted at children. The motivation lies in validating privacy policies to observe compliance with requirements and guidelines provided by privacy laws and regulations, aiming to perceive gaps and understand how a potential lack of transparency from companies can be remedied prior to making the policies available to the user responsible for granting consent. Considering that wearables with activity tracking capabilities (i.e. fitness trackers) collect and process a type of sensitive data, as categorised in Recital 35 of the General Data Protection Regulation (GDPR)[4], this study utilised the privacy policies of these products as main subject of the investigation.

---

sion - Federal Trade Commission (FTC) <https://consumer.ftc.gov/consumer-alerts/2022/03/kurbo-ww-charged-collecting-kids-personal-info-without-parents-permission>

[3] Children's Advertising Review Unit Finds TickTalk Tech in Violation of COPPA and CARU's Privacy Guidelines - CARU <https://bbbprograms.org/media-center/dd/ticktalk-tech-coppa-caru-privacy-guidelines-violation>

[4] Recital 35 | Health Data* - GDPR <https://gdpr-info.eu/recitals/no-35/>

1.3 Research Question

The research questions to drive the study were structured in one main research question and one sub-question as presented below. The main research question drives the primary concern of understanding the core of the problem at hand. The secondary research question guides the investigation further and aims to comprehend additional concerns around the primary concern.

- **RQ:** Do privacy policies for products targeted at children provide clear information based on the requirements of laws and regulations?
  - **Sub-RQ:** Is there a structured process to evaluate the quality of children's privacy policies to assess compliance with requirements of laws and regulations?

1.4 Objectives

The main objective of this research is to understand whether the information provided in privacy policies for products targeted at children are compliant with the requirements of well-established privacy laws. The secondary objective is to propose an audit process that evaluates privacy policies for products targeted at children with the goal of assessing the quality of the information provided to the user and whether the policies do, in fact, meet the requirements from laws and regulations. The study adopts a catalogue of quality criteria to understand how privacy policies are presented to the user (TERRA; VILELA; PEIXOTO, 2022) and proposes a redesign of the criteria from the perspective of children's privacy protection. Additionally, a questionnaire tool is designed to assess these policies based on the questions provided in the new catalogue, generating directives that can assist companies with enhancing the quality of the policies they present to parents and guardians. The third objective of this research is to understand the results generated by the audit process to discuss potential correlations between the compliance level of these privacy policies with regulations guidelines and whether there is any intention from companies not to provide straightforward information to parents and guardians in their policies.

1.5 Structure

From this chapter onward, this document is structured as follows:

Chapter 2 outlines core literary concepts to leverage the comprehension of the topics involved in this study.

Chapter 3 describes the methodology of this research. The methodology guides the process of (i) investigation and definition of scope, (ii) the selection of an existent catalogue to evaluate privacy policies, (iii) the development of an audit process for quality assessment and its artefacts, and lastly, (iv) the evaluation of the proposed audit process and interpret the results.

Chapter 4 presents the main contribution of this research, which is the audit process to assess quality in children's privacy policies. As part of the main contribution, the secondary contributions are the Children's Privacy Policy Quality Criteria Catalogue and the Audit Questionnaire, both described as part of the audit process.

Chapter 5 outlines the evaluation of the proposed audit process by assessing the privacy policies of two products targeted at children.

Chapter 6 encompasses the discussion of the conducted evaluation and the concerns raised throughout its execution.

Chapter 7 presents the conclusion of the contributions presented in this study, the limitations and threats to validity, the related work, and lastly, the future work that can be extended from this research.

2 Literature Review

2.1 Wearables and Children

2.1.1 Wearables in Health

In the year 2022 alone, the market for wearable medical devices was estimated to be worth $30.1 billion[1]. Realms such as the fitness one holds a significant share of consumer wearables; this sector is where the this type of technology continues to thrive due to the public's desire to achieve peak fitness levels for health, sport, and oftentimes aesthetics reasons. Several known wearables from companies such as Fitbit, Garmin, Samsung, and Apple offer wrist worn devices that allow monitoring of the body during a variety of exercises, sleep, etc. This type of wearable can be viewed as a lifestyle device (FERNáNDEZ-CARAMéS; FRAGA-LAMAS, 2018).

However, the growing adoption of wearable technologies (e.g. smart watches) not only helps to passively gather significant volumes of health-related data but also paves the way for using the device to enable remote diagnostic capabilities in child and adolescent psychiatry. For instance, remote diagnosis and management of psychiatric diseases in children via wearables has been crucial, given the current shortage of trained mental health professionals (WELCH et al., 2022). Other works can be found in the psychiatry field such as the one by Sequeira et. al, where mobile and wearable devices displayed potential capabilities for utilising this type of technology to aid in self-monitoring and objective data collection, leading to potential predictions of depressive moods in children and adolescents (SEQUEIRA et al., 2020).

This category is expected to continue its considerable expansion due to its impact on reducing health expenditure via cutting labour costs, equipment purchases, and use of hospital space. Its ongoing evolution continues to shape and change the way medicine is practised and the way healthcare is often provided. With fitness trackers, for example, users are now able to measure personal metrics such as blood pressure, heart rate, sugar levels, vital signs, oxygen levels, body temperature, and other personal metrics, thereby improving their lifestyles. With significant adoption from users and the massive amount of daily personal data these devices consume, issues regarding privacy and other ethical concerns come to light that stakeholders tend to often ignore (ANAYA et al., 2017).

[1] Global Wearable Medical Devices Market Forecast - <https://market.us/report/wearable-medical-devices-market/>

2.1.1.1 Activity Trackers for Children

There has been significant growth and interest in commercially available wearable activity trackers for the past decade. Studies have examined the validity and reliability of wearable devices to measure key metrics such as steps, distance travelled, active minutes, and energy expenditure. The studies also highlight the potential impact of activity trackers in promoting physical activity levels as adoption among children increases (MACKINTOSH et al., 2019).

Though there is an observed active physical activity promotion via wearable activity trackers for older groups, few devices have youth as a specific target, given that wearable fitness trackers specifically designed for children (e.g. KidFit, Fitbit Ace, and Garmin Vivofit Jr.) have been gradually becoming more available. Given that self-monitoring has been identified as a useful behaviour change technique for enhancing awareness of, and potentially stimulating change in, physical activity levels, wearable activity trackers could play an important role in improving awareness of children's physical activity levels among parents and the children themselves (MACKINTOSH et al., 2019).

Overall, the main research agenda around youth and tracking technologies – as in wider self-tracking research – generally questions the potential value of informatics to support health and well-being, and presents concerns related to privacy and control (LYALL, 2021). Although the fitness tracking tools offer general health-related benefits for users, there is an inherently unpredictable challenge regarding the threats to data privacy and security, and that concern increases when the data in question comes from minors. These threats exist due to the possibility of ubiquitous collection of large amounts of data in real time that generate overly detailed user behaviour patterns (e.g. when people eat, sleep, exercise or go home from work), while also tracking users' locations and whereabouts. Recent devices and applications collect both personal information and health data in order to provide "a quantified self for their users," which becomes especially risky when the companies in custody of users' data potentially violate their privacy and misuse it (FIETKIEWICZ; ILHAN, 2020).

2.2 Privacy Engineering

The United States' National Institute of Standards and Technology[2] defines privacy as the "assurance that the confidentiality of, and access to, certain information about an entity is protected"[3], and in the context of technology, often comes with a set of high level principles, oftentimes clustered in sector-specific and generic guidelines and regulations. In regards to data privacy, it can be described as a way to empower users to make their own decisions about who can process their data and for what purpose[4], with several data processing regulations to be found worldwide. In the US, the Federal Privacy Council (FPC) Fair Information Practice

[2]National Institute of Standards and Technology (NIST) <https://www.nist.gov/>
[3]Privacy - Glossary - NIST (US) <ttps://csrc.nist.gov/glossary/term/privacy>
[4]GDPR - Data Privacy <https://gdpr.eu/data-privacy>

Principles (FIPPs)[5] and the California Consumer Privacy Act (CCPA); in the EU, the General Data Protection Regulation (GDPR)[6]; and in Brazil, the General Personal Data Protection Law (LGPD)[7]. In this context, eliciting privacy requirements implies translating these high-level, abstract principles into operational requirements, joining them with requirements derived from end-user concerns and other stakeholders' expectations, and solving the potential conflicts that may arise (NOTARIO et al., 2015).

The concept of privacy engineering addresses an overall lack of generalisation in existing approaches; shortage in efforts to integrate different subdisciplines' techniques and tools; the need to evaluate proposed approaches in different social, organisational, technical, and legal contexts; and concrete challenges emerging from the evolution of engineering practices, technical architectures, legal frameworks and social expectations (Gürses; del Alamo, 2016). The research of privacy protection in computer science has generated a vast array of solutions, even though the implementation of these findings into practical engineering has been significantly hindered. Reports of privacy violations and technology companies' failure to comply with basic data protection requirements continue to grow annually and have become commonplace, suggesting that we are far from applying privacy design know-how in practice (Gürses; del Alamo, 2016). Nevertheless, when it comes to privacy, a data breach is only one concern among many. Subtle engineering decisions that ignore users' privacy needs may have far-reaching consequences (Gürses; del Alamo, 2016).

An ongoing challenge for researchers centres around privacy-friendly systems, and most efforts have followed three prominent approaches. **Privacy by architecture** describes an effort to minimise the collection or inference of sensitive information by unintended parties, typically service providers coupled with developed technologies that enhance privacy by applying techniques that establish constraints on data collection and processing (Gürses; del Alamo, 2016). **Privacy by policy**, one that aims at *"protecting consumer data from accidental disclosure or misuses and facilitating informed choice options"* (Gürses; del Alamo, 2016), which translates to reinforcing measures to ensure compliance with principles of data protection laws regarding information systems. These requirements may include *11specifying and notifying users of the purpose of collection; limiting collection and use to this purpose; being transparent about additional recipients of the data; and providing users access to their data for verification, correction, and deletion"* (Gürses; del Alamo, 2016). Proposed technologies include policy specification languages, policy negotiation and enforcement mechanisms, and design techniques to improve the readability of privacy policies.

Privacy by interaction focuses primarily on socio-technical designs[8] that improve users'

[5] FPC - Fair Information Practice Principles (FIPPs) <https://www.fpc.gov/resources/fipps/>

[6] General Data Protection Regulation (GDPR) - Official Legal Text - <https://gdpr-info.eu>

[7] General Personal Data Protection Law (LGPD) - Official Legal Text <https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#ementa>

[8] *Describes the application of social and ethical requirements to human-computer interaction, software and hardware systems.*

agency with respect to privacy in social settings; this approach captures privacy matters that arise between peers or in a workplace due to the introduction of information systems (Gürses; del Alamo, 2016). It differs from the privacy by policy approach, for example, by not primarily concerning itself with how organisations collect and process data. (Gürses; del Alamo, 2016). Lastly, **privacy by design** (PbD) is rooted in providing organisations with a means to successfully achieve both privacy and functional requirements from the very beginning stage of the software development's life-cycle (Cavoukian; Kursawe, 2012). It can be described through seven core principles that leverage the framework to interoperate with other controls for specific domains and use case scenarios. These principles suggest that the design process of systems require *"minimal data collection processes and proper notice and consent interactions"* (HADAR et al., 2018). PbD has stepped under the spotlight in recent years as data protection regulations escalate their demand for software engineers to inherit PbD principles throughout the development and apply data protection solutions in their projects, taking main technological developments as a vessel to provide solutions (Martin; Kung, 2018). The General Data Protection Regulation[9] (GDPR) in the European Union, for example, embodies the core principles of this approach.

The low adherence to privacy requirements can provoke media backlash and lead to costly legal trials around privacy breaches, and distrust caused by these breaches is possibly the one real blemish on the image of technology companies such as Google or Facebook (SPIEKERMANN, 2012). A company's branding stands as one of its most valuable asset, as well as the most difficult to build and likely the most costly to maintain. Hence, brand managers should be keen to avoid privacy risks. Several companies have been caught in the cross-hairs of public privacy scandals, with repercussions that can often be detrimental once the reports reach the media and require major intervention on the company's end to remediate mapped breaches (REBELO; VALENçA; LINS, 2021).

It is known that the consequences of poor privacy design decisions lies in the inevitable impact on global infrastructures, such as cloud services and mobile networks. Reports of tech giants such as Apple, Google, and Amazon indicate malicious collection of location information gathered by their respective mobile devices from Wi-Fi hotspots and through their cloud-connected devices (REBELO; VALENçA; LINS, 2021) (Gürses; del Alamo, 2016). The importance of adhering to responsible privacy engineering practices can be seen in works such as Ayala-Rivera et al. with the operalisation of GDPR requirements through the proposal of *GuideMe*, a 6-step systematic approach to be implemented within the organisation's software system for supporting elicitation of requirements by interspersing GDPR data protection demands with privacy controls to properly meet these obligations (AYALA-RIVERA; PASQUALE, 2018). Li et al. also outline in their work the operalisation of GDPR requirements combined with a GDPR tool that verifies these requirements, can be executed automatically, which checks privacy requirements in various elements in an AWS cloud infrastructure (LI et al., 2020).

[9]General Data Protection Regulation (GDPR) - Official Legal Text - <https://gdpr-info.eu>

Despite improvements regarding privacy matters in the corporate field, the core challenge for designing privacy requirements is to get organisations' management to adopt them within the development strategy. Their active involvement in the corporate privacy strategy is crucial as personal data continues to be the asset at the core of most companies' business models (SPIEKERMANN, 2012). Managing personal data means optimising its strategic use, quality, and long-term availability (SPIEKERMANN, 2012).

2.2.1 Children's Rights by Design

The Children's Rights by Design (CRbD) standard encompasses the design, development and execution of online services or products used by children, in accordance with the CRC provisions, with the primary consideration of children's protection and best interests (HARTUNG, 2020). Generally speaking, provisions that do not explicitly mention children but are especially important for them, such as the principles of privacy by design and privacy by default as well as data protection impact assessments, should be featured prominently. Although these privacy principles do not focus specifically on children, regulations like the GDPR having privacy by design as their backbone can potentially mitigate some of the concerns with control over personal data (SIMONE; LIEVENS, 2017).

The inclusion of the principles of data protection by default and data protection by design in the GDPR, for example, are regulatory innovations that can boost children's privacy protection if properly implemented and with the targeted users in mind (SIMONE; LIEVENS, 2017). In the EU, the GDPR implements Privacy by Design (PbD) to integrate these fundamental concerns within the process with prevention in mind. PbD contains seven pillars that centralise the need for privacy to become an organization's default mode of operation: (i) proactive not reactive; (ii) privacy as the default setting; (iii) privacy embedded into design; (iv) full functionality; (v) end-to-end security; (vi) visibility and transparency; and (vii) respect for user privacy (VALENçA et al., 2022). Article 8 of the official GDPR text highlights the conditions applicable to a child's consent in relation to information society services[10], affirming that *"where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child"* and determining the controller as responsible for making *"reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology"* (GENERAL DATA PROTECTION REGULATION (GDPR), 2019). Lastly, Recital 38 of GDPR states additional requirements regarding children's data as follows:

> *"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights*

[10] Art. 8 - GDPR | <https://gdpr-info.eu/art-8-gdpr/>

> *in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."*

As Livingstone outlines, there are still conceptual and practical issues that should, ideally, be based on a stronger empirical basis than exists at present; these concern children's media literacy, the harm that the regulation seeks to avoid, and the implied nature of family relations (LIVINGSTONE, 2018).

It is important to highlight that, in the case of misuse of children's personal data taking place in the digital environment and, consequently, having their rights violated, the greatest onus should not be on parents due to their consent or the lack of media literacy. The main accountability in this regard should lie with the unequal power relationship between companies (REBELO; VALENçA; LINS, 2021) and families, coupled with the general inability to understand the complexity and opacity of digital relationships and business models in this area (HARTUNG, 2020).

2.2.2 Privacy Concerns in Wearables

Despite the benefits fitness trackers offer, their use can involve privacy risks. In order to profit from the benefits, users need to accept the challenges and threats; data privacy and security are certainly main concerns, since wearable technology encourages collection, storage, and sharing of health-related data, which is often considered much more sensitive than the usual name-gender-age information (FIETKIEWICZ; ILHAN, 2020). Some of the elicited concerns involve the ability of users opting to share their data with their tracker's manufacturer and/or the manufacturer's affiliates, meaning they must compromise their privacy to benefit from the third-party services and/or organisations and to expose their fitness data on online social networks for self-presentation (VELYKOIVANENKO et al., 2021). In addition to possible data breaches, earlier studies show that existing machine-learning techniques are capable of inferring users' sensitive information based on the data provided by fitness trackers, as observed in several media reports disclosing privacy and security-related incidents involving fitness wearables (VELYKOIVANENKO et al., 2021).

There is scientific interest in users' behaviours when sharing their personal fitness information and the privacy concerns resulting from the collection, aggregation, and sharing of these pieces of data (FIETKIEWICZ; ILHAN, 2020). A study by Füster et al. examined threats in terms of confidentiality, integrity, and availability of the information handled by wearables (fitness trackers). For threats to confidentiality, the study determined most wearables are vulnerable to three types of attacks: eavesdropping (unauthorised real-time interception of a confidential

communication); traffic analysis (monitoring traffic exchanged between wearable devices and their base and/or server); gathering information transferred between the device and its base (usually via smartphones) (FúSTER et al., 2023). It also expanded the main attacks that threaten the integrity of these devices, such as attacks that modify the information transmitted by the device, replaying attacks of packets to impersonate the user's identity or corrupt data, and masquerading attacks (where the attacker impersonates an authenticated device in order to intercept data or inject false information within the system). These vulnerabilities are reported to be due to weak authentication methods or the absence of encryption in communications between devices (FúSTER et al., 2023).

2.3 The Role of Privacy Policies

As we navigate further into a data-driven society, the privacy landscape evolves accordingly, with significant attempts to protect privacy and security led by businesses, in some cases fuelled by the recently growing social outrage and academic literature. Naturally, this is reflected in, and supplemented by, privacy law and policy. The GDPR, for instance, is a legislation that applies internationally, including even non-European entities that process personal data of EU consumers (BECHER; BENOLIEL, 2020). Studies have shown that online consumers often face difficulties understanding the terms and conditions they must agree to when signing up for the majority of services. Other works have reported that the main inhibitor to the user's comprehension derives from the type of language these privacy policies adopt (BECHER; BENOLIEL, 2020). Additionally, other findings have reported that privacy policies are often riddled with legal and technical jargon that makes them rather inaccessible to the average user (IBDAH et al., 2021). Regarding the readability of privacy policies, some studies delve deeper into how quantitative approaches to measure readability as the basis for computer-based approaches can be applied to privacy statements and assessing the minimum requirements for being able to understand this type of text (KRUMAY; KLAR, 2020). As highlighted by Ermakova et al.:

> *"It should be in the interest of companies that technical Internet knowledge of its users is strengthened. In all cases, perceived Internet literacy, which is being positively influenced by actual Internet literacy in all cases as well, was shown to have a positive impact on how the readability of PP was perceived".* (ERMAKOVA et al., 2014)

As a requirement, the GDPR establishes that companies must use "clear and plain" language when communicating with the intended users. This plain language[11] requirement branches into a few elements, one of which is consent. Consent is one of the core elements of information

[11] *The plain language movement aims to ensure that legal texts are written in a readable manner so that laypeople can read and easily understand them (BECHER; BENOLIEL, 2020).*

privacy laws, with a significant part of privacy law and policy grounded in it (BECHER; BENOLIEL, 2020). The need for meaningful and freely given consent is reaffirmed within the policies outlined in the GDPR and the LGPD, serving as one of the crucial pillars of these regulations.

Readability, therefore, plays a huge part in what is considered a guided, clear form of consent. Consent suggests that we have control over the processing of our personal data, but also implies that we have a significant choice that enables understanding of data processing practices of controllers (SIMONE; LIEVENS, 2017);. Consent requires free choice, although if users are interested in signing up for online services or apps, companies usually offer no choice to the user but to conform with their privacy policy (which necessitates granting access and conforming with their data processing practices), or leave it altogether, given that these policies are often built on a take-it-or-leave-it basis. Moreover, users are seldom aware of what they consenting to, as they generally do not read privacy policies due to their complex nature; plus, there are several apps that do not even have privacy policies (SIMONE; LIEVENS, 2017). On the other hand, informed consent mandates services to clearly notify end-users of what kind of data is stored on their device and for what specific purpose. Furthermore, any and all users must be granted the opportunity to refuse solicited access, once assessed that it is not strictly needed for the main operation of its corresponding service (KRETSCHMER; PENNEKAMP; WEHRLE, 2021).

Additionally, if users are sufficiently aware of the consequences of data usage, privacy concerns are, for the most part, significantly mitigated. However, it is rather unlikely that users can provide firms with meaningful and informed consent, as they are generally unaware of the companies' data collection practices (BECHER; BENOLIEL, 2020). Users are also unable to fully grasp and absorb the immense amount of information involved. Ultimately, users may suffer from cognitive biases and limited attention span, which might prevent them from taking any issues into consideration.

3 Research Method

This research was structured as a **descriptive case study** with the goal of proposing an audit process. The theoretical basis utilised for this case study follows the design based on describing, analysing and interpreting events that justify the reasoning behind specific phenomena in a real life context (BLOOMBERG, 2019) (YIN, 2019). This process aims to assess, from a quality perspective, the content of privacy policies from gadgets for children. As part of the audit, the role of companies concerning the transparency of their data handling practices is also discussed. The approach has the goal of deriving conclusions from different perspectives to enable compliance-driven directives through the implementation of the proposed process. By combining grey literature, gadget reviews from Mozilla's *Privacy Not Included*[1] and literature review, we were able to conduct a comprehensive analysis on potential informative gaps caused by lack of clarity in privacy policies provided by the companies behind the gadgets. The main criteria for selecting the devices was rooted in the gadgets' high ratings coupled with their activity/fitness tracking capabilities (due to the nature of the data that can be collected).

Fig 1 outlines all phases encompassed in this study. In Phase 1, the main focus was investigating gadgets that were designed for children and selecting the ones that would undergo further analysis. Phase 2 comprises the execution of the initial quality evaluation based on the selected reviews. Phase 3 encompasses the development of the quality audit process and its artefacts: the quality criteria catalogue and the audit questionnaire tool. Phase 4 describes the final evaluation of the audit process.

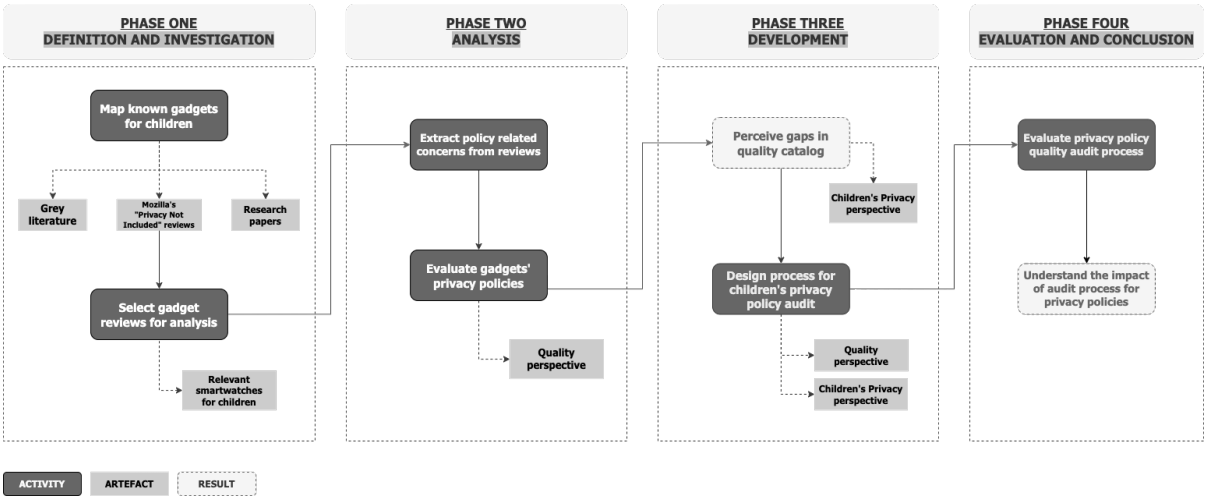

Figure 1 – *Research Phases*

[1] Privacy Not Included - Mozilla <https://foundation.mozilla.org/en/privacynotincluded/>

3.1 Research Phases

3.1.1 Phase 1 - *Definition and Investigation*

The first phase involved the process of conducting a broader online research regarding general privacy concerns for children, eventually redirecting our focus to the gadgets segment. As we filtered through the results, we mainly concentrated on what would be defined as *wearables* within the gadgets scope, taking into account the relevance of the product and whether or not it was discontinued. Additionally, the literature background served as a basis for the conceptual pillars required to analyse the elements we extracted from the reviews of each gadget, reinforcing our main goal of comprehending how privacy is outlined for the end user and where the observed gaps exist. The investigation branched into two separate stages, as outlined below.

Stage one described the process of searching the Internet for children-focused products that presented concerns regarding privacy matters. Initially, most of the investigation redirected to results associated with smart toys, which was not the focus of this particular research. Detailed queries can be found in Appendix A.1. By refining our query (presented below), we were able to identify products that were more aligned with our scope within Mozilla's privacy guide called *Privacy Not Included*, which has the goal of helping users shop smartly and safely for products that connect to the internet [2]. The reasons to select this guide provided by Mozilla are the following: (i) the reviews conducted by Mozilla follow a structured methodology (see Section 3.1.2 for details) and provide resources for justify their claims; (ii) the fact that there were products targeted at children among Mozilla's reviews; (iii) the observed correlation between the products that served as subject of the reviews and the studies found throughout the literature review; (iv) the concerns raised in the reviews regarding the lack of straightforward information in products' privacy policies.

Stage two encompassed the selection of reviews among those listed in Privacy Not Included. For products that are marketed for children, the following categories were identified: *Toys & Games, Drones, eReaders for Kids, Fitness Trackers for Kids, STEM/Coding Learning Kits, Tablets for Kids*. For this study, the categories were grouped into three macro categories:

- *Toys* INCLUDES 'Toys & Games', 'Drones', 'STEM/Coding Learning Kits';
- *eReaders* INCLUDES 'eReaders for Kids';
- *Gadgets* INCLUDES 'Fitness Trackers for Kids', 'Tablets for Kids'.

A total of **28 reviews** for these products were identified across the categories listed by Privacy Not Included. For the purposes of this study, the macro category **Gadgets** was chosen and products selected for analysis included 'Fitness Trackers for Kids' and the additional

[2]*Privacy Not Included - Mozilla <https://foundation.mozilla.org/en/privacynotincluded/>

category of 'Wearables'. Although no 'Wearables for Children' category was identified, it was observed that the 'Wearables' category was included in all reviews under the 'Fitness Trackers for Kids'.

Those constraints resulted in a list of **six** products. Among the results, four products had an additional warning tag labelled as 'privacy not included', which indicates privacy concerns were raised throughout the review process [3]. That indicator served as our deciding factor for the final list, which is outlined in Fig. 3. An overview of each product can be found in Appendix A.2.

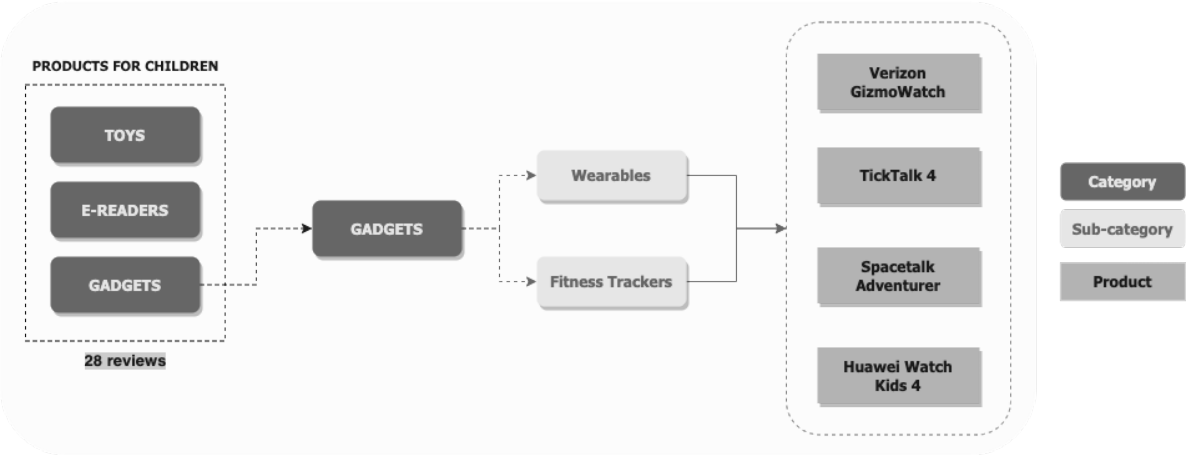

Figure 2 – *'Privacy Not Included' Reviews Selection*

3.1.2 **Phase 2** - *Analysis*

This second phase covered the process of extracting information from the product reviews that were selected in the previous phase, followed by a quality assessment of their privacy policies. Initially, a thorough review was conducted to understand the elements involved in Mozilla's results, such as the sources behind their claims and a better understanding of how they generated their own methodology[4] to execute the process. As highlighted in their Methodology page, *"the way we approach our research here (...) is from the viewpoint of a consumer but with a bit more time and expertise"* with decisions based on *"top selling products that are highly rated across a variety of consumer product websites such as Consumer Reports, Wirecutter and CNET"*, which served as a relevant perspective to this study. The pillars of Mozilla's methodology for the review process include the following:

- **Permissions**: "If it is possible the device could snoop on you if it were hacked, leaked, or not working correctly; to determine this, we check product websites and the Google Play Store or the Apple App Store to check on the permissions requested by each app

[3] Privacy Not Included - Our *Privacy Not Included warning label <https://foundation.mozilla.org/en/privacynotincluded/about/why/>

[4] Privacy Not Included - About our Methodology <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/>

to determine whether the device and its app uses a camera, microphone, or tracks your location" (MOZILLA, 2022a);

- **Privacy**: "Evaluate the publicly available privacy documentation provided by each company for each product. This includes privacy policies, privacy pages, and FAQs. We attempt to determine (1) what kind of information is generally collected by a product, including personal, body-related, and social; (2) how the data is used by the company, (3) how you can control your data, including how you can access and delete your data; (4) the known track record of a company for protecting user data; (5) if the product can be used offline; (6) and whether the privacy policy is user-friendly" (MOZILLA, 2022a);
- **Minimum Security Standards**: "Mozilla established a set of Minimum Security Standards we determine should be met by any manufacturer developing connected products. We evaluated each product on our list against five criteria: Encryption; Security updates; Strong passwords; Vulnerability management; Privacy Policy" (MOZILLA, 2022a);
- **Artificial Intelligence**: "We evaluate whether or not a product uses artificial intelligence. We defined AI as: automated technology that makes decisions for you and/or changes continually based on your user data" (MOZILLA, 2022a);
- ***Privacy Not Included Warning Labels**: "A product will earn the *Privacy Not Included warning label if it receives two or more warnings from us on the following criteria: how the company uses the data it collects on users[5]; how users can control their data[6]; what is the company's known track record of protecting users' data?[7]; if we can not confirm if the product meets our Minimum Security Standards[8]" (MOZILLA, 2022a).

In order to have a better understanding of each piece of information provided in these reviews, we performed a fine extraction to better categorise the data we aimed to analyse. For visualisation purposes, the data was re-categorised under umbrella sections to understand how the disclosure of data handling was detected. Elements such as the accessibility of the privacy policy, the collection and retention of personal data, and whether the company or the product had any certifications related to protecting children's privacy were taken in consideration to serve as input for the subsequent research steps. Lastly, conclusions drawn by Mozilla's reviews were interpreted as potential pros and cons, combined with their analysis of the companies' track records. The complete extraction spreadsheet can be found here.

[5]About our Methodology - How does the company use this data <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/#how-does-company-use-this-data>

[6]About our Methodology - How can you control your data? <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/#how-can-you-control-your-data>

[7]About our Methodology - What is the company's known track record of protecting users' data? <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/#company-track-record>

[8]About our Methodology - Minimum Security Standards <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/#minimum-security-standards>

The following step utilised the extraction spreadsheet as input to further identify these privacy gaps by delving into each individual Privacy Policy. Our main motivator was the common issue found in the reviews of users being recurrently presented with a confusing list of policies that could come across as contradictory or dubious, along with difficulties regarding where the privacy policy could be accessed at. To further assess these concerns, we utilised a privacy policy quality criteria catalogue proposed by Terra *et al.* which has the general goal of supporting *"requirements engineers and analysts/developers/testers to assess the consistency between the privacy policy, requirements document, and the application behavior since the treatment performed by the application must be consistent with the one described in the policy and in the requirements document; privacy policy writers to improve the completeness of the policy; and end-users to assess whether the policy follows good practices"* (TERRA; VILELA; PEIXOTO, 2022). The original catalogue in its entirety can be found in Attachment B.1.

For each product, a privacy policy quality evaluation was executed based on the catalogue previously mentioned. The goal was to answer all the questions with a combination of the spreadsheet information and the individual privacy policy of each product being investigated in this study. This approach was chosen in order to guarantee consistency and even delve into greater detail than Mozilla's reviews alone could potentially offer. The assessment for each product can be found in Appendix A.3.

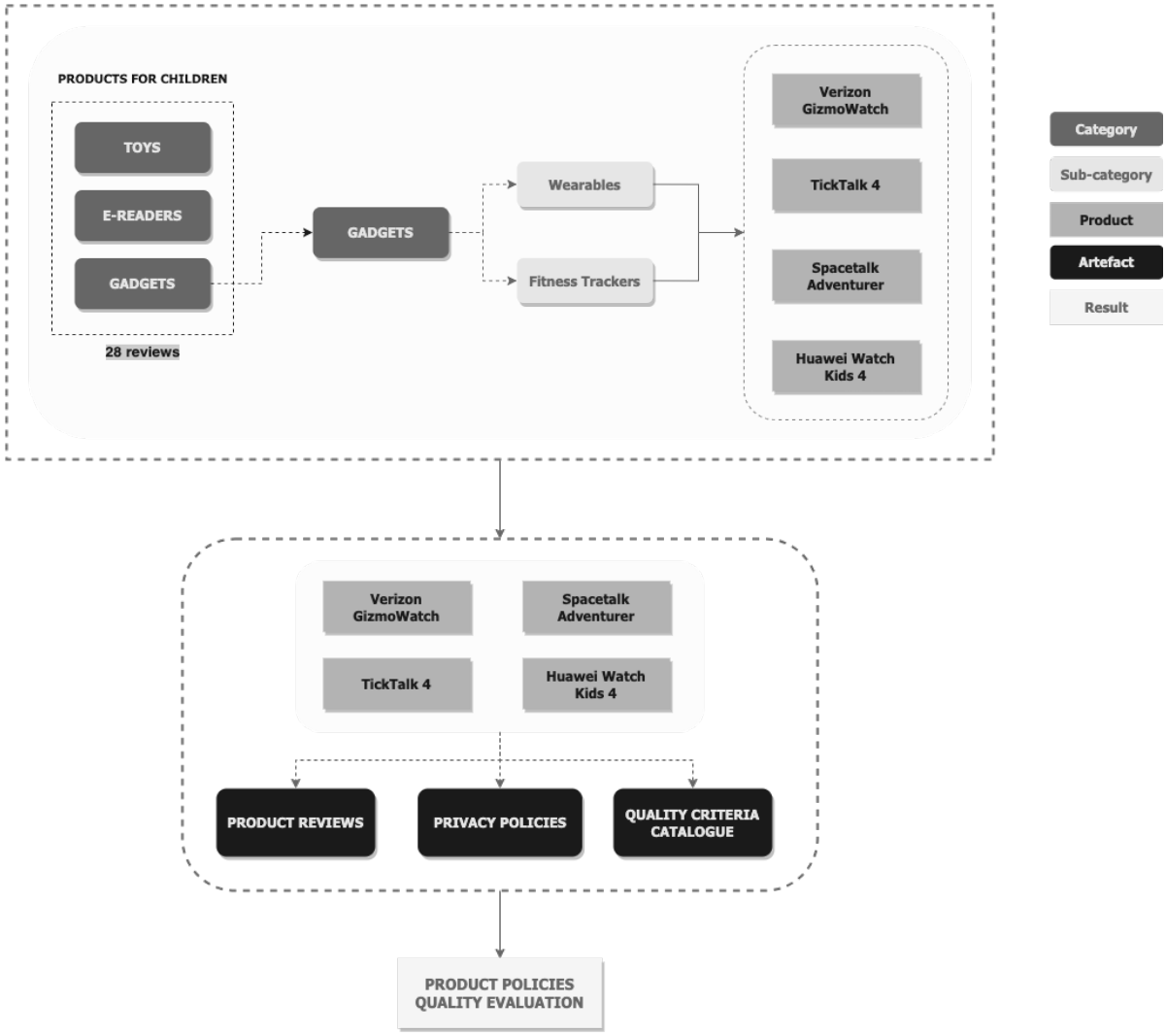

Figure 3 – *Product Policies Evaluation*

3.1.3 **Phase 3** - *Development*

3.1.3.1 Children's Privacy Policy Quality Catalogue

This third phase commenced with an analysis of the preliminary privacy policy quality assessment to understand how the existing catalogue could be adapted to assertively cover children's privacy concerns. By revisiting literature and reading through regulations such as the GDPR[9], CCPA[10], COPPA[11], and PIPEDA[12], we identified the requirements for the kind of information these policies should provide and whether the existing quality catalogue (TERRA; VILELA; PEIXOTO, 2022) allowed us to answer these requirements satisfactorily. Subsequently,

[9] General Data Protection Regulation (GDPR) <https://gdpr-info.eu/>

[10] California Consumer Privacy Act (CCPA) <https://oag.ca.gov/privacy/ccpa>

[11] Children's Online Privacy Protection Rule (COPPA) <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

[12] The Personal Information Protection and Electronic Documents Act (PIPEDA) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>

that same existing catalogue was adapted in order to have the child user as the core subject.

The process included adding newly developed questions which stemmed from noted observations that occurred in the previous phase (see Section 3.1.2), e.g. details about certifications, and where the privacy policy is located on the product's official website; adapting existing questions to specify concerns with the child user; removing additional questions that were not pertinent to this particular study and its ultimate purpose.

3.1.3.2 Quality Audit Questionnaire

The proposed quality catalogue for children's privacy policy was transformed into a questionnaire in order to operationalise the assessment. Inspired by the works of Alaya-Rivera *et al.*, we established a methodology to outline the main structure of the questionnaire flow based on each of the categories that was established in the comprehensive catalogue list, where each category and answer have their own respective weight. Just as the aforementioned research aimed to act on a perceived lack of guidance to understand which requirements should be operationalised and implemented to support compliance (AYALA-RIVERA; PASQUALE, 2018), the questionnaire is a tool aiming to generate results that incentivise companies to improve the readability of their privacy policies from a quality perspective.

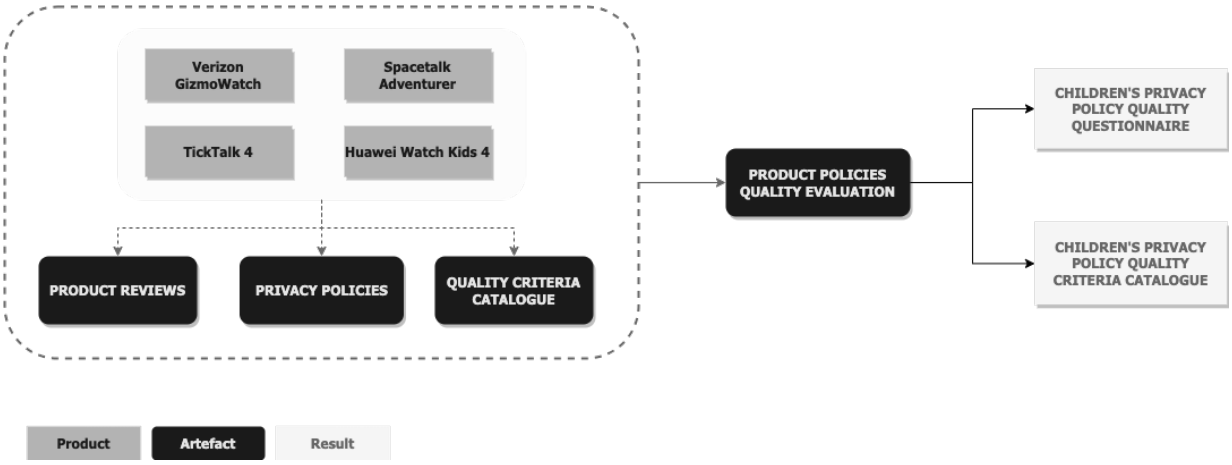

Figure 4 – *Children's Privacy Policy Assessment Artefacts*

3.1.3.3 Quality Audit Process Proposition

Lastly, the artefacts previously developed were combined to generate a quality audit process concerning the privacy policy for products aimed at children. The basis for determining how crucial this process would be was heavily based on prioritising Children's Privacy by Design (as detailed in Chapter 2) and inherent requirements to comply with children-specific regulations. Both the children's privacy policy quality catalogue and the quality audit questionnaire were visualised as part of a broader audit process that comprised the actions required by the company to improve the quality of their privacy policy prior to reaching the end user (i.e. parents and guardians). The audit process flow is described in Fig. 5.

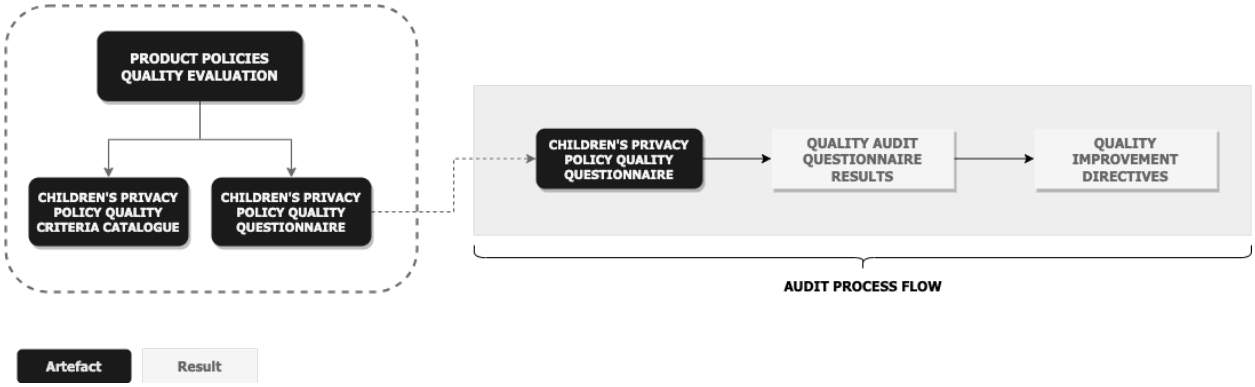

Figure 5 – *Children's Privacy Policy Audit Flow*

3.1.4 **Phase 4** - *Evaluation and Conclusion*

3.1.4.1 Quality Audit Process Evaluation

The final phase comprises an evaluation of the audit process for assessing privacy policy quality proposed in Phase 3.1.3. In order to make the assessment, the other two products listed in Mozilla's 'fitness trackers for children' category were selected (see 3.1.1) and the quality audit questionnaire was applied to each one, as illustrated in Fig. 6. These two products, unlike the others within the same category, were not granted a 'Privacy Not Included' warning label in their Mozilla reviews, therefore the evaluation aims to validate Mozilla's verdict by performing an assessment of each of their privacy policies. A compilation of the results includes the compliance percentage generated by the tool, the amount of points achieved in each category, and lastly, a list of directive actions based on the submitted responses.

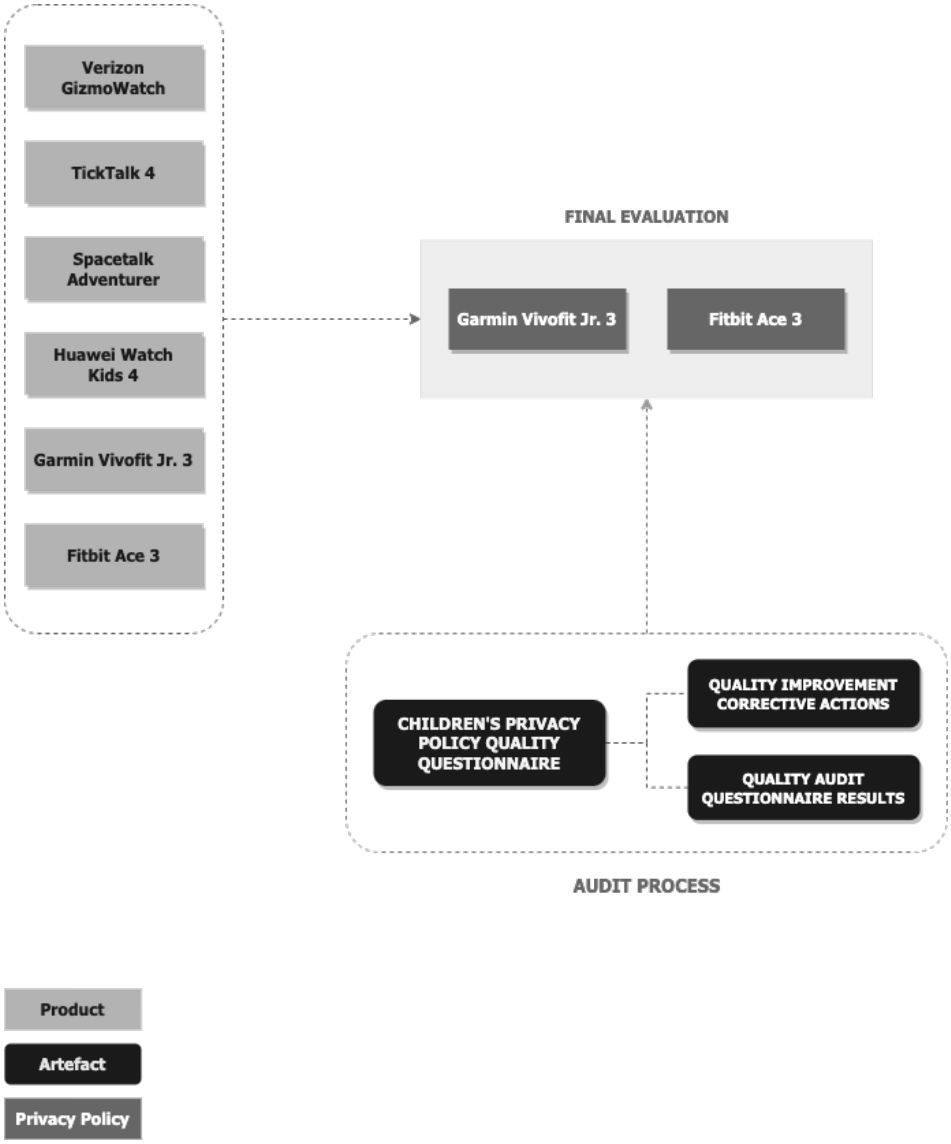

Figure 6 – *Audit Process Evaluation*

The evaluation was followed by a discussion surrounding incongruities in privacy policies and compliance with privacy laws and regulations potentially impacting companies' reputations. It also expanded into the correlations between the observed gaps in their privacy policies and the company's history regarding the protection of users' privacy, subsequently delving into their track record regarding transparency and due diligence to remediate privacy or data breaches in the face of public reports in the media.

4 Results

This chapter comprises the results obtained from the studies performed under the structure presented in Phase 3 as illustrated in Section 3.1 of Chapter 3. The presented sections are outlined to disclose (i) **the proposed catalogue for children's privacy policy quality assessment**; (ii) **the questionnaire for assessing the children's privacy policy quality**; and lastly, (iii) **the privacy policy quality audit process**. These results are discussed in the subsequent chapters to ensure the correlation between each element involved in the development of the proposed audit process and the impact on the privacy policy based on the evaluation.

4.1 Children's Privacy Policy Quality Audit

This section encompasses the elements that describe the proposed quality audit for children's privacy policies, structured to outline the development of (i) **the children's privacy policy quality criteria catalogue**; (ii) **the quality audit questionnaire**; and lastly, (iii) **the privacy policy quality audit**, which includes all the aforementioned artefacts.

4.1.1 Children's Privacy Policy Quality Criteria Catalogue

The catalogue presented below is a direct result of the quality assessment performed beforehand with the quality catalogue proposed by Terra et al. concerning the privacy policies from the wearables that were previously discussed (see Appendix A.3). By performing the earlier assessment, it was observed that, not only were the questions mainly focused on the application itself and not on the product, the term 'user' was applied more generically. The new set of questions intends to place the child user as the primary focus and the core of the concerns by adapting the original catalogue (TERRA; VILELA; PEIXOTO, 2022) to fit the children-focused scope. Additional questions to identify compliance elements related to the handling of health data and information concerning certifications regarding protection of children's privacy from certified boards were also included. Questions regarding accessibility from the original catalogue were disregarded. The questions are grouped in the same five categories: *User Experience*, *User Consent and Permission*, *Rights of Data Subject*, *Privacy Policy Content* (subdivided in Child User Privacy Concerns, Security Concerns, and Data Concerns), and *Privacy Policy Changes*. The catalogue in its entirety is presented in Table 1.

- **User Experience**: This category aims to assess what kind of experience the company is offering once the user comes in contact with the product or its main product page. Concerns such as whether the privacy policy can be easily understood by the user, as well as where the user can find the privacy policy on the product page, are included.

- **User Consent and Permission**: This category has the goal of understanding what kind of information the privacy policy provides regarding the parents' and guardians' abilities when it comes to granting (or not) permission for collecting the child user's data upon using the product.
- **Rights of Data Subject**: This category is focused on assessing how the privacy policy outlines the ways in which the child user and/or parents and guardians can access their personal information, and whether the company provides communication channels to address concerns of this nature.
- **Privacy Policy Content**: This category aims to understand how informative and descriptive the privacy policy is regarding the data handling process of the child user's data, what and how it is collected, whether the company actively engages in sharing information with external parties, and what kind of information there is concerning data security measures.
- **Privacy Policy Changes**: This last category aims to understand how the company handles any changes to their privacy policy and what their chosen methods are for informing parents and guardians if the policies previously consented to have been modified in some capacity, how frequent these changes are, and whether the company presents a version history of the document.

User Experience	
Criteria	**Description**
Is the Privacy Policy readily available for access by the parent or guardian?	*This aims to understand whether the user is redirected to the Privacy Policy at first contact with the product (via website or device).*
How easy is it for the parent or guardian to access the Privacy Policy?	*Where the Privacy Policy can be found and accessed by the parent or guardian (i.e. website, application, device).*
Where is the Privacy Policy of this product located at?	*To grant further accessibility to the Privacy Policy, parents and guardians should be able to access a direct link to the policy from the main product page or the website's navigation bar.*
Is the document properly translated to all the languages the device supports?	*The current policies must be properly written and translated to all languages that the device's services are available in.*
Does the document present a readability level compatible with its targeted audience?	*The Privacy Policy needs to be read and understood by whomever is responsible for granting consent; it should be clear and straightforward. Technical jargon should be avoided.*

User Consent and Permission	
Criteria	**Description**
What is the chosen method for giving parents and guardians the option to agree with the Privacy Policy's terms?	*The user must check pertinent boxes that grant conformity with the presented policies (i.e. opt-in forms).*
Is the parent or guardian able to choose whether to agree with the Privacy Policy or not?	*The product must clearly express that the parents and guardians are allowed to disagree with any of the presented policies in the Privacy Policy.*
Is the parent or guardian allowed to select what kind of information they grant for collection?	*It is advised that parents and guardians be able to select what type of information they allow or do not allow to be collected by the device's integrated services. They should be assured that, if consent has not been granted, the data will not be collected and/or retained.*
Rights of Data Subject	
Criteria	**Description**
Does the privacy policy inform whether the parent or guardian is able to access their personal data?	*It is advised that parents and guardians should be allowed to view their stored data directly from the device in order to confirm the accuracy and integrity of the collected information.*
Does the privacy policy specify the child user's rights?	*The privacy laws grant users with a set of rights. It is advised that the policy clearly states the ones regarding children's personal data.*
Does the Privacy Policy provide ways to contact the company?	*Ideally, there should be a Contact section or page redirecting the user to multiple ways to reach the company for the purpose of handling privacy concerns.*
Privacy Policy Content	
Child User Privacy Concerns	
Criteria	**Description**
Is the Privacy Policy built on the assumption that the parent or guardian has granted consent upon purchase of the product?	*It is expected that a parent or guardian manually confirms their agreement with the informed policies presented for data collection; it should not be implied that consent has been granted from the purchase of the device alone.*
Are there explicit mentions of compliance with laws and regulations in the Privacy Policy?	*The Privacy Policy must explicitly state whether users are covered by privacy laws (regional or otherwise) and which ones.*
Does the Privacy Policy expand and provide details on concerns regarding children's privacy?	*It is advised that the policy expands clearly on matters that are directly related to children's privacy and how they are handled within the device's services.*

For the children-specific Privacy Policy, does the company refer to a separate Privacy Policy for additional information?	*In the case of having more than one Privacy Policy, the company should clarify to the parent or guardian if there is additional information in a separate document and where to find it.*
Does the Privacy Policy inform parents and guardians about certifications regarding the protection of children's privacy?	*If the company or the product possesses any certifications from certified boards that reinforce their commitment to protecting children's privacy, it is advised that those be included in the Privacy Policy.*
Security Concerns	
Criteria	**Description**
Does the Privacy Policy clearly specify if the device makes use of any tool or external service?	*If any external services or tools are used, regardless of the purpose, it is advised to attach links that redirect to these third parties' privacy policies.*
Does the privacy policy specify how the child user's data is stored?	*By clearly outlining how the company stores their users' data, it grants them a level of both credibility and accountability; it also reflects the company's concerns with security matters, depending on which services they choose for the purpose.*
Does the privacy policy specify any measures adopted by the company to ensure the basic principles of data security are met?	*This criteria aims to assess whether the device has any capabilities to ensure the child user data's confidentiality and integrity. For example, if the data storage is encrypted or some IP mask is used.*
Data Concerns	
Criteria	**Description**
Does the policy clearly specify what data is collected from the child user?	*It is fundamental that the Privacy Policy expands on what data will be collected from the child by the device.*
Does the Privacy Policy clearly specify how the child user's data is collected?	*The policy must clearly specify which tools are used to collect data in the device.*
Does the Privacy Policy specify how the company can use the child user's collected data?	*The intents and purposes of collecting children's data should be described in the Privacy Policy.*
Does the Privacy Policy provide information surrounding health data handling?	*In the case of a product that handles sensitive information such as health data, it is advised to include it in the privacy policy.*

Does the Privacy Policy specify whether the child user's supplied data is voluntary or mandatory?	*To assess whether the Privacy Policy is flexible or not, there should be clear mentions of what happens if the user chooses to provide certain types of information or not; for example, there are devices/applications that require enabling access to microphone, GPS, and list of contacts.*
If the child user's data is not provided, does the Privacy Policy mention the consequences upon refusing to provide the requested information?	*If the parent or guardian chooses not to provide the solicited information, the policy should address the consequences of opting to reject the requested consent.*
Does the Privacy Policy specify whether the child user's personal data can be shared or sold to third parties?	*If there are third parties involved, it is required to describe what type of information that is shared, who the third parties are, and the circumstances in which they are shared under the applicable laws. The third parties should be disclosed and their respective Privacy Policies should be available for access.*
Does the policy clearly explain what happens to the child user's data if they opt to delete their account?	*It is fundamental for the Privacy Policy to describe what happens to the user's account information once they choose to delete their data from the device and services.*
Privacy Policy Changes	
Criteria	**Description**
How are changes in policies handled?	*If there are any changes made to the Privacy Policy, the users need to be promptly notified.*
How do the Privacy Policy changes reach the user?	*How are users redirected to changes made in the current version of the Privacy Policy? How does the company make sure the changes reach the user? (i.e. triggering a notification that informs the user about changes in the Privacy Policy with a comparison between versions).*
How frequent are the changes in the Privacy Policy?	*The company should provide a modification date and version history of existing privacy policies.*

Table 1 – *Proposed catalogue to assess children's privacy policy quality*

4.1.2 Audit Questionnaire

In order to operationalise the quality assessment, the catalogue that was previously proposed was redesigned as a front-end system to be used as part of the audit process described in the subsequent section (see 4.1.3) and named *Children's Privacy Policy Quality Audit Question-*

naire. To generate scores and weights, and the corrective measures as part of the results for the questionnaire, the following steps were taken:

Initially, the catalogue was redesigned as an entity relational diagram to understand how each of the categories were related and what kind of action it enabled over another. Weights between 1 and 5 was utilised to perceive the most and least influential category in the catalogue based on the amount of questions in the category and the relationship between the categories. It was understood that the **User Experience** (2) enables **User Consent and Permission** based on the experience given to the user by the company. **User Consent and Permission** then enables (3) **Rights of Data Subject** (4) once the user understands what their given consent entails. The rights they are given and the granted consent is initiated by the **Privacy Policy Content** (5), which holds the crucial array of information. Lastly, the **Privacy Policy Content** triggers **Privacy Policy Changes** (1) in what can be described as a looping relationship.

Fig. 7 outlines the category relationship diagram with its respective weights.

Figure 7 – *ERD for catalogue category weight*

Next, the questionnaire flow was structured following the same order as presented in the proposed catalogue (see Table 1). Due to the nature of the questionnaire, the answers were meant to be generic, apart from exceptions for specific questions. The formats available for answers were: linear scale (0 to 5); 'yes'; 'yes, but not clearly'; 'can't determine'; and 'no'. Each answer has a separate value attributed to it as described in Table 2. For specific questions that required further elaboration in their answers, the text was reformulated for better clarity while preserving the same attributes as the original.

Answer	Points
Yes	5
Yes, but not clearly	3
Can't determine	1
No	0

Table 2 – *Attributed points for questionnaire answers*

Considering the amount of questions within the questionnaire (30 questions) and the maximum amount of points per question (5 points), the goal is to achieve a total of 150 points ($30 * 5 = 150$) by the end of the questionnaire, which equals to a 100% compliance percentage based on the calculation. The amount of points per category equivalent to the intended total sum is described in Table 3.

Category	Points
User Experience	25
User Consent and Permission	15
Rights of Data Subject	15
Privacy Policy Content	80
Changes to Privacy Policy	15
Total	**150**

Table 3 – *Total sum per category*

The final stage concerns the conclusion of the questionnaire once the responses are submitted. Action items will be generated and displayed, coupled with a compliance percentage calculated with the weighted mean of each category, for potential modifications on the current version of the privacy policy. The goal is to provide assertive directives that allow the company to deliver a well-rounded list of policies, while meeting compliance requirements. This compliance guide was developed by compiling a combination of official sources provided by international privacy regulations, articles that were found during the literature review phase of this research (presented in Chapter 2), and useful resources found on the internet. The comprehensive list of resources can be found in the Appendix A.5.

The questionnaire is divided in four screens that represent the flow of the application. Fig. 8 illustrates the initial screen of the tool, displaying a button that allows the user to commence the assessment. Fig. 9 showcases the subsequent screen once the user enters the assessment, displaying the current category and the questions that follow. Fig. 10 illustrates the dashboard presented to the user once the assessment has been finalised with the compliance percentage results. The screen displays the overall compliance percentage, as well as a pie chart with the percentage per category. The user is also able to expand the details of the results to visualise the generated directives. Lastly, Fig. 11 outlines the directives generated based on each incorrect answer and the link to the official source where the guidelines were extracted from (see Appendix A.5 for the list of resources).

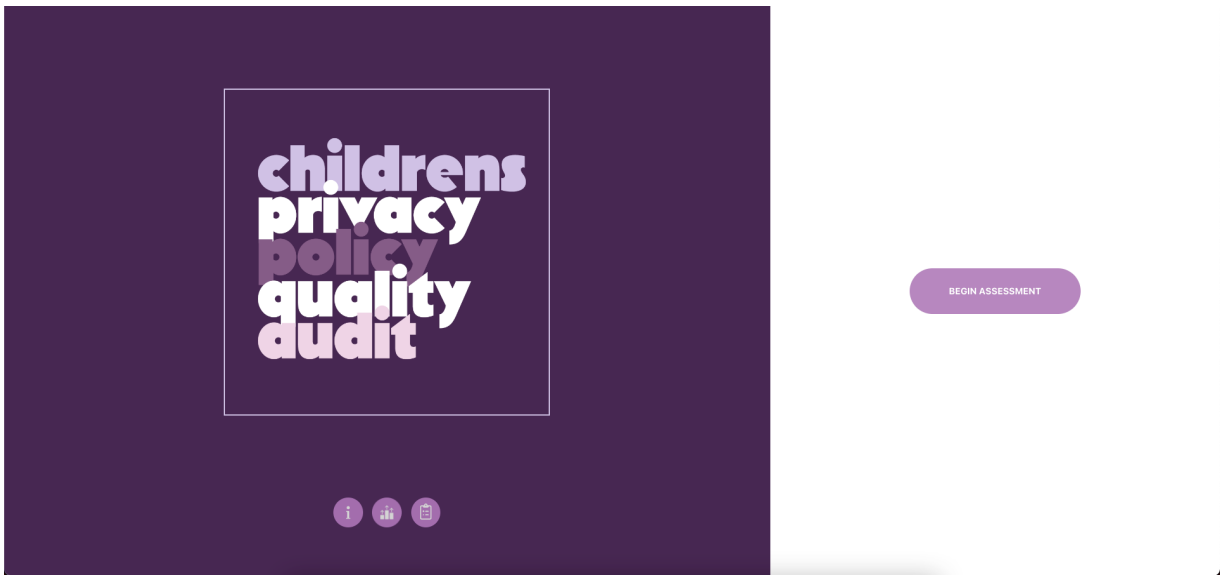

Figure 8 – *Questionnaire: Main Screen*

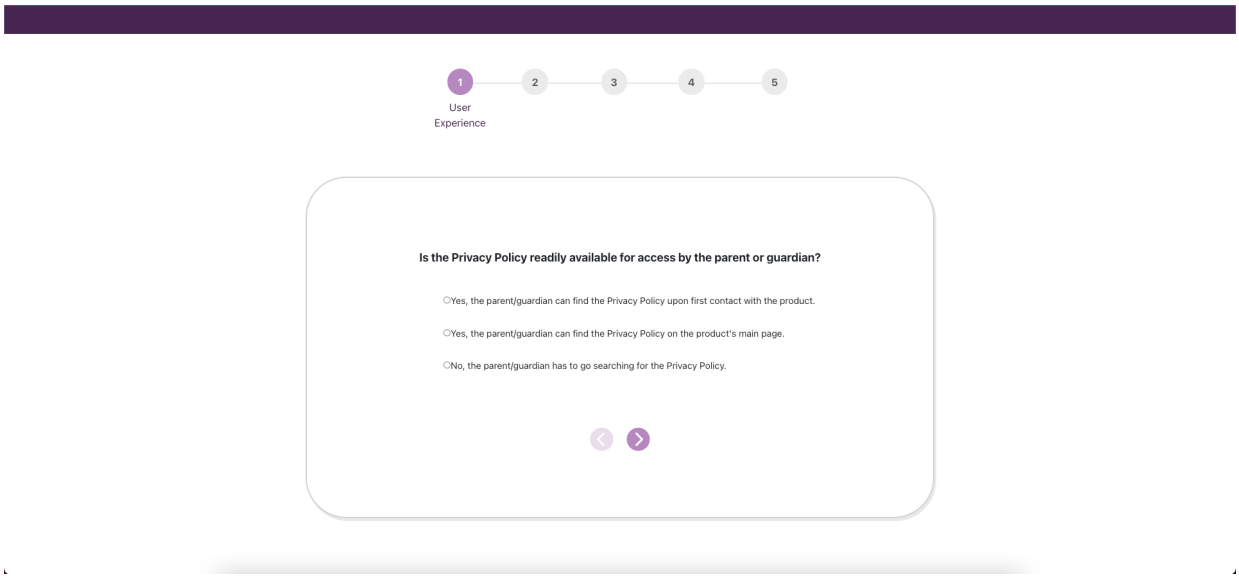

Figure 9 – *Questionnaire: Audit Questions Flow*

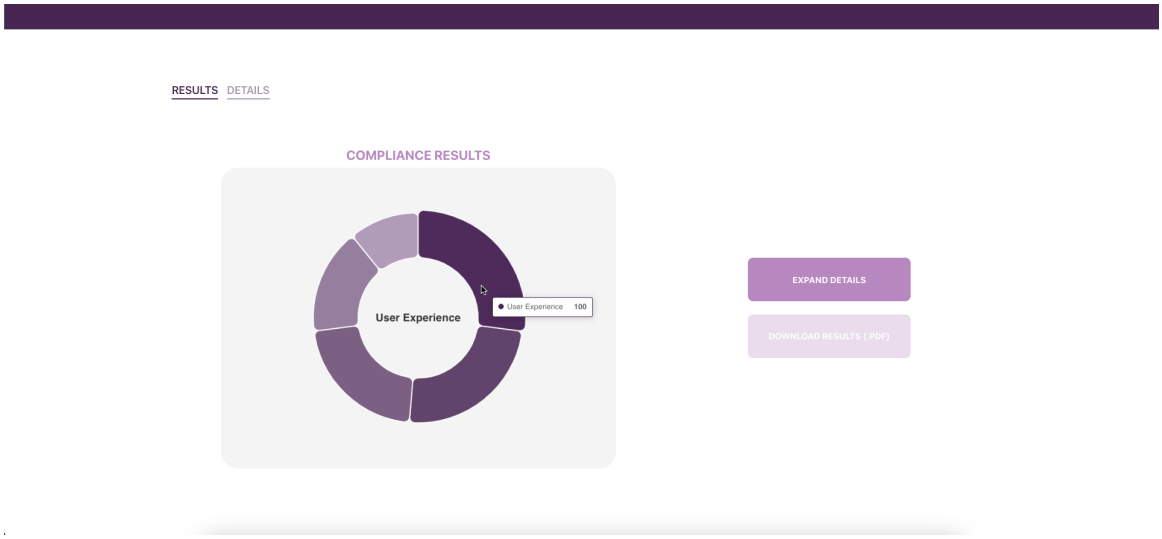

Figure 10 – *Questionnaire: Audit Results Dashboard*

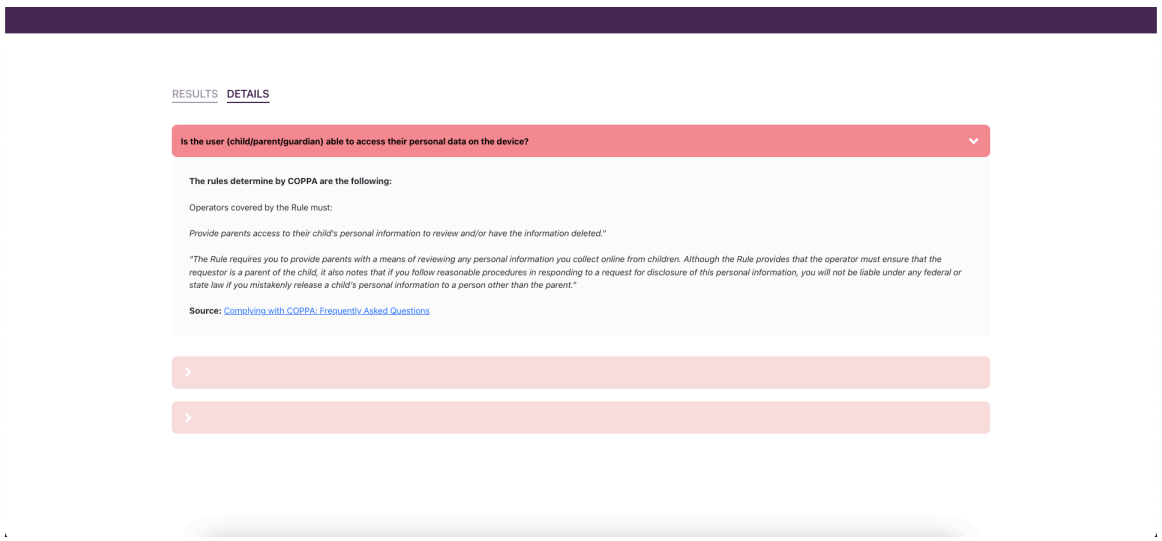

Figure 11 – *Questionnaire: Generated Directives*

4.1.3 Children's Privacy Policy Quality Audit Process

This section describes the quality audit process for privacy policies that concern products aimed at children. The goal of the proposed process is to operationalise the aforementioned quality audit questionnaire, subsequently aiding companies with certifying that the information comprised in their privacy policies is straightforward, and written clearly, and also complies with privacy laws and regulations standards. Fig. 12 illustrates the business model in full.

The three main actors involved in the process are the Company, the Evaluator, and the User, represented by the swimlanes in Fig 12. **Company** represents any company that offers products aimed at children or any individual lawfully considered a minor. **Evaluator** represents the individual responsible for applying the audit questionnaire and delivering the results to the competent entities from the company; this evaluator could be either an internal employee (i.e.

employees from the company's legal/compliance department) or an external individual hired to conduct the assessment. **User** represents the Parent or Guardian responsible for reading through the presented privacy policies upon or prior to product purchase.

Here are the BPMN's input and output for the process:

FROM	TO
Company offers a product with its privacy policy to the user.	*User agrees and accepts the privacy policies in order to use the product.*

4.1.3.1 Stage 1 – *Company*

The first stage illustrates the initial part of the process which comprises the two following tasks:

- **Create Privacy Policy**: company has to create a privacy policy for the product that it is offering to customers.
- **Create children-specific Privacy Policy:** company has to create a separate, dedicated privacy policy to address concerns related to children's privacy.

Once the company has created a privacy policy for the product, the subsequent step is to verify whether or not the product has a dedicated privacy policy addressing children's privacy concerns. If the company does not have the latter, one should be promptly created. The children-specific privacy policy and the main privacy policy should be handed over to the evaluator so they can proceed with the audit.

4.1.3.2 Stage 2 – *Evaluator*

The second stage illustrates the privacy policy audit by the evaluator and it is described in four different tasks and the 'Applying the Audit Questionnaire' subprocess.

- **Read the Privacy Policy**: the evaluator is handed the pertinent privacy policies by the company to conduct a thorough reading. If the company has more than one privacy policy addressing children's privacy, they should be made available to the evaluator as well.
- **Perform Privacy Policy Audit**: the evaluator will commence the ensuing subprocess.

Once the evaluator has conducted a reading of the privacy policies to be audited, they should proceed to execute the audit process by applying the questionnaire (see 4.1.2) on each of the privacy policies that were submitted.

Subprocess: Applying the Audit Questionnaire

The evaluator accesses the Children's Privacy Policy Quality Audit tool and answers all the questions based on the information gathered previously throughout the reading phase. Once all the categories have been responded to, the tool will generate the results based on the inputs given by the evaluator, which include compliance percentage and action items to address any found gaps. Once the evaluator has collected the results, they will return them to the company for the respective entities to apply the corrective measures.

4.1.3.3 Stage 3 – *Company*

The third stage comprises the company's tasks following the results from the quality audit performed in the preceding phase.

- **Obtain Audit Results**: company receives the results from the audit questionnaire that were delivered by the evaluator.
- **Revise Privacy Policy**: company re-evaluates the privacy policy based on the action items provided in the results.
- **Adjust Privacy Policy**: if changes to the privacy policy are required, the company adjusts the privacy policy and returns it to the evaluator for another audit round.
- **Make Privacy Policy Available to Users**: once the changes have been approved, the company notifies the users about changes and makes the policy available to the customers.

The company then revises the privacy policies based on the results that were generated by the questionnaire and collected from the audit performed by the evaluator. If gaps and mismatches are detected as per the answers given and changes to the privacy policy are deemed necessary, the company proceeds to act upon the required modifications by adjusting the policies. Afterwards, the company should return the new version of the privacy policy back to the evaluator for another round of quality audit.

The scenarios to follow are determined by the constraints presented below:

1. If the required modifications are approved after the audit validation and the current version is approved, the company should verify whether this is the first version of the privacy policy or not.
    a) *If the current version is the first version (v1) of the document, the privacy policy should be made available to the public via the company's chosen platforms;*
    b) *If the current version is not the first version (v1), customers/users should be notified that changes were made to an existing privacy policy.*

2. If no changes are required and the current version is approved, the company should verify whether this is the first version of the privacy policy or not.

    a) *If the current version is the first version (v1) of the document, the privacy policy should be made available to the public via the company's chosen platforms;*

    b) *If the current version is not the first version (v1), customers/users should be notified that changes were made to an existing privacy policy.*

4.1.3.4 Stage 4 – *User*

This final stage encompasses the tasks related to the User once they are able to have access to the privacy policy of the product at hand.

- **Reads Privacy Policy**: user has access to the privacy policy provided by the company and reads through the statements;
- **Agrees with Privacy Policy**: user agrees with the privacy policy statements via the method provided by the company.

Once the user accesses the privacy policy and reviews the privacy statements presented by the company, it proceeds to either agree or disagree with the established requirements for the product to operate. Whether the user opts to select the former or the latter (and they should have the option to do either), they can proceed to utilise the product regardless.

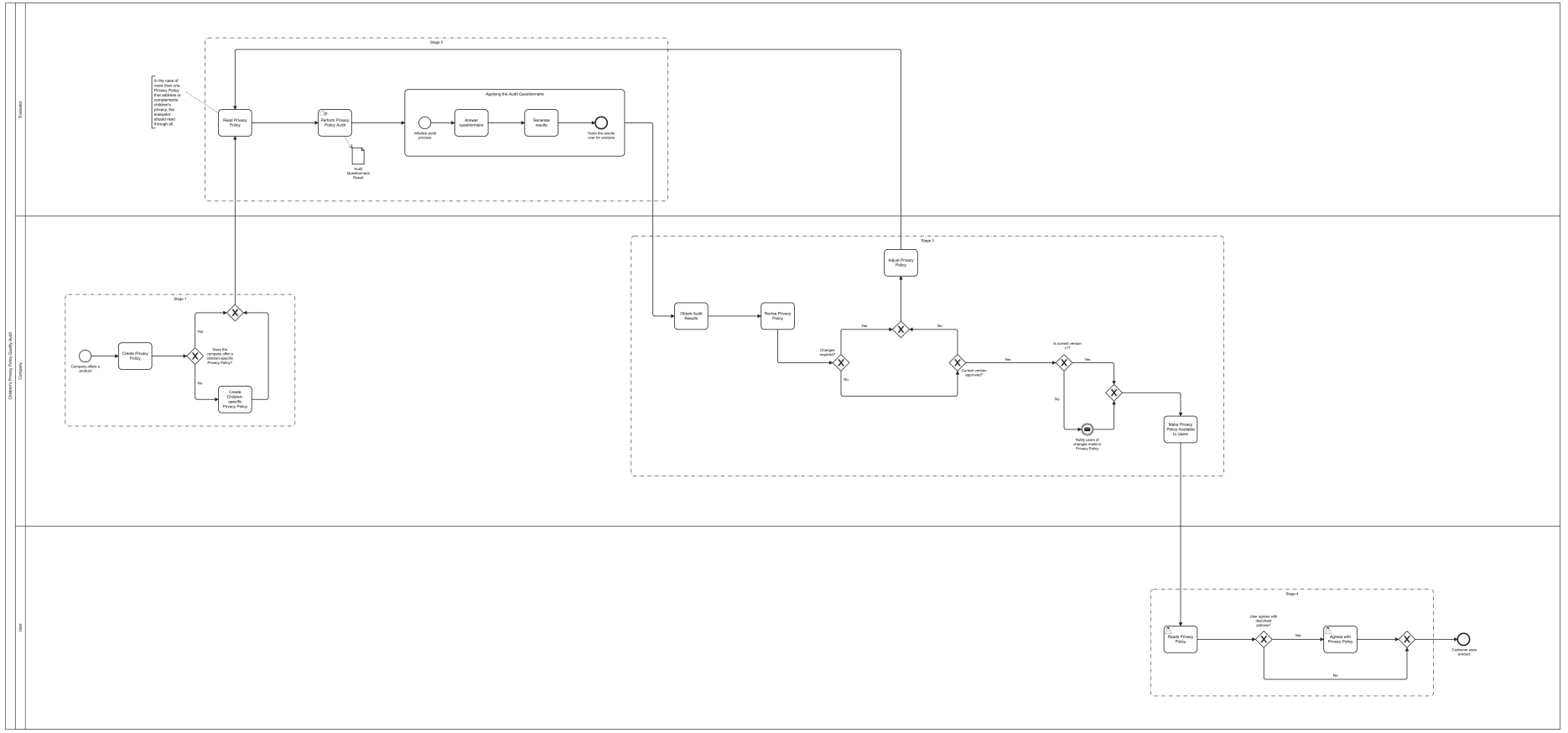

Figure 12 – *BPM model of the proposed quality audit process*

5 Evaluation

This chapter comprises the performed evaluation of privacy policies from products targeted at children by executing the proposed quality audit process as described in Chapter 4 (see Section 4.1.3). The presented sections outline each of the products used for the assessment, the results generated by the audit questionnaire tool, and the recommended directives based on these results.

5.1 Audit Process Evaluation

This section outlines the evaluation which focuses on the initial stages (see Sections 4.1.3.1 and 4.1.3.2) of the audit process. The outputs of the evaluation are a direct result of the audit questionnaire (see Section 4.1.2) and reflect the metrics and directives generated by the tool upon submitting the responses; henceforth, the suggestive directives given to remediate the issue are based on each incorrect answer. The products selected for this evaluation were identified during the investigation process (see Section 3.1.1). Out of the six reviewed products (outlined in Fig. 3), the fitness trackers from Garmin and Fitbit were not granted a 'Privacy Not Included' warning label in their Mozilla reviews.

5.1.1 Case 1: *Garmin*

The first evaluation was conducted using a prominent smartwatch for kids by Garmin, a renowned American company currently headquartered in Switzerland that offers a broad selection of high-end fitness devices. Although there are two separate smartwatches for children listed on the website, their connectivity is established through the same Garmin Jr.[1] app, meaning the assessment could apply to both Garmin Bounce™[2] and Garmin vívofit® jr. 3[3] as it was identified that they share the same privacy policy.

Garmin provides two separate privacy policies: the main privacy policy[4] and the Garmin Jr. App[5] privacy policy. Both these documents were taken into consideration and utilised to execute stages 1 and 2 (see Sections 4.1.3.1 and 4.1.3.2) of the audit process.

The final score for Garmin's policy privacy quality audit indicated a compliance percentage of approximately 63%. It was observed that the privacy policy found its strength in the

[1] Garmin Jr. App <https://play.google.com/store/apps/details?id=com.garmin.android.apps.vivokid&hl=en&gl=US>, <https://apps.apple.com/us/app/garmin-jr/id1122225740>

[2] Garmin Bounce™ <https://www.garmin.com/en-US/p/714945>

[3] Garmin vívofit® jr. 3 <https://www.garmin.com/en-US/p/711488>

[4] PRIVACY POLICY - Garmin <https://www.garmin.com/en-US/privacy/global/policy/>

[5] PRIVACY POLICY FOR GARMIN JR. APP - Garmin <https://www.garmin.com/en-US/privacy/garminjr/policy/>

Privacy Policy Changes category with a score of 13/15 points; despite the significant numbers, the category has the lowest weight among all. The category of *Rights of Data Subject* also presented a score of 13/15 points, though unlike the aforementioned one, it weighs significantly on the final result. For the most relevant category, *Privacy Policy Content*, Garmin's privacy policies scored a total of 50/80 points, around 62.5% of the total category points. *User Consent and Permission* had a total score of 11/15 points, resulting in around approximately 73% of the category points. *User Experience*, however, came in last with 6/25 possible points for the category, which represents 24% of the category sum.

A compilation of the directives returned by the tool for each incorrect answer is presented below.

User Experience

- Q: Is the Privacy Policy readily available for access by the parent or guardian?
- A: No, the parent/guardian has to go searching for the Privacy Policy.
  - Directive: *The official six-step compliance document from the FTC states that, for COPPA compliance, companies must: "make those links clear and prominent. Consider using a larger font or a different color type on a contrasting background. A fineprint link at the bottom of the page or a link that isn't distinguishable from other links on your site won't do the trick. To comply with COPPA, your privacy policy should be clear and easy to read. Don't add any unrelated or confusing information."*
    (Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business - Federal Trade Commission (FTC)[6])

- Q: Where is the Privacy Policy of this product located at?
- A: In the footer of the website.
  - Directive: *Generally speaking, the Privacy Policy link should be available in the footer and anywhere where personal information is collected. However, for compliance with the Children's Online Privacy Protection Rule (COPPA), the common practice of placing a link for the Privacy Policy at the bottom of the page won't suffice. The link should be evidently available for the user. "Include a link to your privacy policy on your homepage and anywhere you collect personal information from children. If you operate a site or service directed to a general audience, but have a separate section for kids, post a link to your privacy policy on the homepage*

[6]Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business - FTC <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>

of the kids' part of your site or service."
(Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business - Federal Trade Commission (FTC)[7] | Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[8])

User Consent and Permission

- Q: What is the chosen method for giving parents or guardians the option to agree with the Privacy Policy's terms?
- A: Can't determine.
  - Directive: *The section "I know that the Rule requires that I provide a direct notice to parents before I collect personal information from children. What information must be included in the direct notice?" in FTC's official FAQ for COPPA compliance outlines the requirements for giving parents a direct notice and the circumstances to which they apply.*
    (Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[9])

Rights of Data Subject

- Q: Does the privacy policy inform whether the parent or guardian is able to access their personal data?
- A: Yes, but not clearly.
  - Directive: *The rules determined by COPPA are the following: "Operators covered by the Rule must:*
    Provide parents access to their child's personal information to review and/or have the information deleted."
    "The Rule requires you to provide parents with a means of reviewing any personal information you collect online from children. Although the Rule provides that the operator must ensure that the requestor is a parent of the child, it also notes that if you follow reasonable procedures in responding to a request for disclosure of this

[7]Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business - Federal Trade Commission (FTC) <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>

[8]Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

[9]Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

personal information, you will not be liable under any federal or state law if you mistakenly release a child's personal information to a person other than the parent."
(Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[10]***)***

Privacy Policy Content

- Q: Does the Privacy Policy inform parents and guardians about certifications regarding the protection of children's privacy?
- A: No.
  - Directive: *The Children's Online Privacy Protection Act (COPPA) includes a provision enabling industry groups or others to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule. List of currently approved Safe Harbor organizations (in alphabetical order):*

    • Children's Advertising Review Unit (CARU)
    • Entertainment Software Rating Board (ESRB)
    • iKeepSafe
    • kidSAFE
    • Privacy Vaults Online, Inc. (d/b/a PRIVO)
    • TRUSTe

    (COPPA Safe Harbor Program - Federal Trade Commission (FTC)[11]***)***

- Q: Does the privacy policy specify any measures adopted by the company to ensure the basic principles of data security are met?
- A: No.
  - Directive: *Here is how regulations address the principles of data security:*

    • GDPR (Art.5, Ch.2)
    1. Personal data shall be:
    (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational

[10] Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>
[11] COPPA Safe Harbor Program - Federal Trade Commission (FTC) <https://www.ftc.gov/enforcement/coppa-safe-harbor-program>

measures ('integrity and confidentiality').

• COPPA
"COPPA requires you to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. Minimize what you collect in the first place. Take reasonable steps to release personal information only to service providers and third parties capable of maintaining its confidentiality, security, and integrity. Get assurances they'll live up to those responsibilities. Hold on to personal information only as long as is reasonably necessary for the purpose for which it was collected. Securely dispose of it once you no longer have a legitimate reason for retaining it."

(Art. 5 – GDPR[12] | Children's Online Privacy Protection Rule ("COPPA")[13])

- Q: Does the Privacy Policy clearly specify how the child user's data is collected?
- A: Yes, but not clearly.
  - Directive: *Regarding data collection, COPPA defines the following criteria for compliance:*

    A description of the personal information collected and how it's used. Your policy must describe:
    - the types of personal information collected from children (for example, name, address, email address, hobbies, etc.);
    - how the personal information is collected — directly from the child or passively, say, through cookies;
    - how the personal information will be used (for example, for marketing to the child, notifying contest winners, or allowing the child to make information publicly available through a chat room); and
    - whether you disclose personal information collected from kids to third parties. If you do, your privacy policy must list the types of businesses you disclose information to (for example, ad networks) and how they use the information.

    (Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[14] | Children's Online Privacy Protection Rule ("COPPA")[15])

[12] Art. 5 – GDPR <https://gdpr-info.eu/art-5-gdpr/>
[13] Children's Online Privacy Protection Rule ("COPPA") - FTC <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
[14] Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>
[15] Children's Online Privacy Protection Rule ("COPPA") - FTC <https://www.ftc.gov/legal-library/browse/

- Q: Does the Privacy Policy provide information surrounding health data handling?
- A: No.
  - Directive: *For products that process health data, the privacy policy should address how the data of that kind is handled by the device and/or service, preferably citing legal resources the company is complying with. GDPR defines health data as a special category of personal data and outlines in Recital 35 that "personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject."*

    (Recital 35 – GDPR**[16]**)

- Q: Does the Privacy Policy specify whether the child user's supplied data is voluntary or mandatory?
- A: Yes, but not clearly.
  - Directive: *The section "I know the COPPA Rule is triggered by the collection of personal information from children, but the information I collect at my site or service is voluntary, not mandatory. Does COPPA still apply?" in the official FTC FAQ for COPPA states:*
    "Yes. The Rule governs the online collection of personal information from children by a covered operator, even if children volunteer the information or are not required by the operator to input the information to participate on the website or service. The Rule also covers operators that allow children publicly to post personal information. Finally, the Rule defines "collection" to include the passive tracking of children's personal information through a persistent identifier, and not just active collection. See 16 C.F.R. § 312.2 (definition of "collection")."

    (Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)**[17]**)

- Q: If the child user's data is not provided, does the Privacy Policy mention the consequences upon refusing to provide the requested information?
- A: No.

rules/childrens-online-privacy-protection-rule-coppa>

[16] Recital 35 – General Data Protection Regulation (GDPR) <https://gdpr-info.eu/recitals/no-35/>

[17] Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

  - Directive: *COPPA determines that "the parent can review or have deleted the child's personal information and refuse to permit its further collection or use. You must also state the procedures for doing so". Additionally, the privacy policy should clearly "state that the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so".*

    (Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[18])

- Q: Does the policy clearly explain what happens to the child user's data if they opt to delete their account?
- A: Yes, but not clearly.
  - Directive: *As per the compliance requirements established by COPPA, the user should be informed of their rights to delete information from the eligible services.*

    "What information must I include in my online privacy policy?
    Section 312.4(d) of the Rule identifies the three categories of information that you must disclose in your online privacy policy:
    • The name, address, telephone number, and email address of all operators collecting or maintaining personal information through the site or service (or, after listing all such operators, provide the contact information for one that will handle all inquiries from parents);
    • A description of what information the operator collects from children, including whether the operator enables children to make their personal information publicly available, how the operator uses such information, and the operator's disclosure practices for such information; and
    • That the parent can review or have deleted the child's personal information and refuse to permit its further collection or use. You must also state the procedures for doing so."

    (Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[19])

[18]Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

[19]Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

5.1.2 Case 2: *Fitbit*

The second evaluation was conducted with Google-owned Fitbit, an American company that provides a wide range of fitness devices for several age groups. Unlike Garmin, Fitbit only has one activity tracker targeted at children on their website, the Fitbit Ace 3, which this assessment will focus on. The connectivity for the device is achieved through the Fitbit App[20] and applies to all available devices regardless of age group.

Fitbit also provides two separate privacy policies: the main privacy policy[21] and the Fitbit Privacy Policy for Children's Accounts[22]. Both of these documents were taken into consideration and utilised to execute stages 1 and 2 (see Sections 4.1.3.1 and 4.1.3.2) of the audit process.

The final score for Fitbit's policy privacy quality audit indicated a compliance percentage of approximately 77.9%. Similar to what was observed for Garmin (see Section 5.1.1), Fitbit also provides relevant information regarding the changes in their privacy policies, with a score of 13/15 points for the *Privacy Policy Changes* category. For both *User Consent and Permission* and *Rights of Data Subject*, Fitbit scored a total of 15/15 points in two of the most relevant categories. For *Privacy Policy Content*, Fitbit's privacy policies scored a total of 60/80 points, around 75% of the total category points. Lastly, *User Experience* presented a total score of 13/25 points, with an average of 52% of the category sum.

A compilation of the directives returned by the tool for each incorrect answer is presented below.

User Experience

- Q: Is the Privacy Policy readily available for access by the parent or guardian?
- A: No, the parent/guardian has to search for the Privacy Policy.
  - Directive: *The official six-step compliance document from the FTC states that, for COPPA compliance, companies must: "make those links clear and prominent. Consider using a larger font or a different color type on a contrasting background. A fineprint link at the bottom of the page or a link that isn't distinguishable from other links on your site won't do the trick. To comply with COPPA, your privacy policy should be clear and easy to read. Don't add any unrelated or confusing information."*

  (Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business - Federal Trade Commission (FTC)[23])

[20] Fitbit: Health & Fitness <https://play.google.com/store/apps/details?id=com.fitbit.FitbitMobile>, <https://apps.apple.com/us/app/fitbit-activity-calorie-tracker/id462638897>

[21] Fitbit Privacy Policy <https://www.fitbit.com/global/us/legal/privacy-policy>

[22] Fitbit Privacy Policy for Children's Accounts <https://www.fitbit.com/global/us/legal/kids-privacy-policy>

[23] Children's Online Privacy Protection Rule: A Six-Step Compliance Plan

- Q: Where is the Privacy Policy of this product located at?
- A: In the footer of the website.
  - Directive: *Generally speaking, the Privacy Policy link should be available in the footer and anywhere where personal information is collected. However, for compliance with the Children's Online Privacy Protection Rule (COPPA), the common practice of placing a link for the Privacy Policy at the bottom of the page will not suffice. The link should be evidently available for the user. "Include a link to your privacy policy on your homepage and anywhere you collect personal information from children. If you operate a site or service directed to a general audience, but have a separate section for kids, post a link to your privacy policy on the homepage of the kids' part of your site or service."*

    (Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business - Federal Trade Commission (FTC)[24] | Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[25])

Privacy Policy Content

- Q: Does the Privacy Policy inform parents and guardians about certifications regarding the protection of children's privacy?
- A: No.
  - Directive: *The Children's Online Privacy Protection Act (COPPA) includes a provision enabling industry groups or others to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule. List of currently approved Safe Harbor organizations (in alphabetical order):*

    • *Children's Advertising Review Unit (CARU)*
    • *Entertainment Software Rating Board (ESRB)*
    • *iKeepSafe*
    • *kidSAFE*
    • *Privacy Vaults Online, Inc. (d/b/a PRIVO)*
    • *TRUSTe*

for Your Business - FTC <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>

[24]Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business - Federal Trade Commission (FTC) <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>

[25]Complying with COPPA: Frequently Asked Questions - FTC <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

(COPPA Safe Harbor Program - Federal Trade Commission (FTC)[26])

- Q: Does the Privacy Policy clearly specify if the product makes use of any tool or external service?
- A: Yes, but not clearly.
  - Directive: *Detailing how third parties play a part in the privacy policy will vary from one regulation to the other. There are different stances based on what needs to be covered by the company.*

    • General Data Protection Regulation (GDPR)
    'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data; (Art.4, Ch.1)

    • California Consumer Privacy Act (CCPA)
    ""Categories of third parties" means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party.

    If any of those elements are to be identified upon reading the Privacy Policy, it should promptly comply with the requirements from COPPA:
    "Name each third party operator, such as an advertising network or social network plug-in, that collects or maintains children's personal information through your site or service. For each, include a name and contact information (address, telephone number, and email address). If more than one is collecting information, it's okay to give contact information for only one as long as that company will respond to all inquiries from parents about your site or service's practices. Even so, you still have to list all third parties in your privacy policy."

    (Art. 4 – GDPR[27] | California Consumer Privacy Act (CCPA)[28] |Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[29])

[26]COPPA Safe Harbor Program - Federal Trade Commission (FTC) <https://www.ftc.gov/enforcement/coppa-safe-harbor-program>
[27]Art. 4 – GDPR <https://gdpr-info.eu/art-4-gdpr/>
[28]California Consumer Privacy Act (CCPA) <https://oag.ca.gov/privacy/ccpa>
[29]Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

- Q: Does the Privacy Policy specify how the child user's data is stored?
- A: No.
  - Directive: *From COPPA: "Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use."*
    "The Rule specifically states that operators should retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. As the Commission noted in the 1999 Statement of Basis and Purpose, "if a parent seeks to review his child's personal information after the operator has deleted it, the operator may simply reply that it no longer has any information concerning that child.""

    (Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[30])

- Q: Does the privacy policy specify any measures adopted by the company to ensure the basic principles of data security are met?
- A: Yes, but not clearly.
  - Directive: *Here is how regulations address the principles of data security:*

    • GDPR (Art.5, Ch.2)
    1. Personal data shall be:
    (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

    • COPPA
    "COPPA requires you to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. Minimize what you collect in the first place. Take reasonable steps to release personal information only to service providers and third parties capable of maintaining its confidentiality, security, and integrity. Get assurances they'll live up to those responsibilities. Hold on to personal information only as long as is reasonably

[30] Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

necessary for the purpose for which it was collected. Securely dispose of it once you no longer have a legitimate reason for retaining it."

(Art. 5 – GDPR[31] | Children's Online Privacy Protection Rule ("COPPA")[32])

- Q: If the child user's data is not provided, does the Privacy Policy mention the consequences upon refusing to provide the requested information?
- A: No.
  - Directive: *COPPA determines that "the parent can review or have deleted the child's personal information and refuse to permit its further collection or use. You must also state the procedures for doing so". Additionally, the privacy policy should clearly "state that the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so".*

  (Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC)[33])

[31] Art. 5 – GDPR <https://gdpr-info.eu/art-5-gdpr/>

[32] Children's Online Privacy Protection Rule ("COPPA") - FTC <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

[33] Complying with COPPA: Frequently Asked Questions - Federal Trade Commission (FTC) <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

6 Discussion

6.1 Understanding the Privacy Policy Quality Audit

This chapter discusses the results of the quality audit process evaluation outlined in Chapter 5, aiming to expand the discussion around the level of transparency in privacy policies for wearables targeted at children. The potential impact of the raised concerns in the delivery of these policies to parents and guardians is also analysed. The discussion assesses how the audit can assist companies to assertively deliver a group of privacy-related policies with a significant level of quality and transparency, and most importantly, in a compliance-driven way. Ultimately, the process has the goal of reassuring that the data handling practices of health-related information and children's privacy concerns are transparent to the user, aiming to prevent future data breaches that result in public reports in the media.

6.1.1 Garmin

For this case, it was observed that although Garmin provides sufficient information to the recipient, it fails to grant easy and direct ways for users to access their privacy policies. The results concerning user experience highlight that Garmin, similar to other companies, places the link to their 'Privacy' section in the footer of their website, making it harder for parents and guardians to find it on the website. The GDPR simply states in Art. 12 that information should be *"concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child"*[1], when COPPA delivers much clearer directives concerning where these resources should be placed, stating that the links should be clear and prominent with *"a larger font or a different color type on a contrasting background"*; Additionally, the compliance guideline establishes that *"a fineprint link at the bottom of the page or a link that isn't distinguishable from other links"*[2] will not suffice to draw the attention of the reader. It was also noted that, despite providing multiple versions of their main privacy policy in other languages, Garmin's policy document concerning children's policy is only available in English.

In regard to rights of data subject and user consent, both privacy policies fail to expand on details concerning how users can actually agree with the proposed terms and access their information by providing only loose statements surrounding where the personal data of both parents/guardians and children can be accessed across the main policy document. The concern

[1] Art. 12 GDPR - *Transparent information, communication and modalities for the exercise of the rights of the data subject* <https://gdpr-info.eu/art-12-gdpr/>

[2] Federal Trade Commission (FTC) - *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>

for the protection of children's personal data increases once it is observed that Garmin has no explicit mention of any practices regarding data security and integrity, indicating that there is no way to determine whether they follow requirements specified in Art. 5 of GDPR and COPPA in this regard.

> *Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); processed in a manner that ensures appropriate security of the personal data,including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*
> – **Art. 5 - GDPR**

> *COPPA requires you to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. Minimize what you collect in the first place. Take reasonable steps to release personal information only to service providers and third parties capable of maintaining its confidentiality, security, and integrity. Hold on to personal information only as long as is reasonably necessary for the purpose for which it was collected. Securely dispose of it once you no longer have a legitimate reason for retaining it.*
> – **Children's Online Privacy Protection Rule ("COPPA")**

Details on how the child's data is collected, through the connected application or the device itself, are either not divulged or vaguely stated, similar to what happens if the parent or guardian opts to either refuse permission for any data collection or delete their information from any of the services. There is also unclear information as to whether the data supply from the child user is voluntary or mandatory, as Garmin appears not to clarify whether choosing not opting in implies opting out. Although Garmin solely manufactures health and fitness related products, there are no sections in either privacy policy dedicated to how they process and handle health data as described in the Recital 35[3] of the GDPR.

No reference to certifications for the products by any of the COPPA Safe Harbor enabled organisations were found. Although it is not necessarily an impediment for purchase, this magnifies the concerns as to how committed the company is to really protecting children's privacy. Furthermore, Garmin appears to concern itself with ensuring that changes in their current policies reach the parents and guardians through their communication channels, requiring that the latter are aware of these modifications and agree to them.

[3] Recital 35 - Health Data - GDPR <https://gdpr-info.eu/recitals/no-35/>

6.1.2 Fitbit

The evaluation for Fitbit yielded results similar to the findings for Garmin regarding the experience provided to the user for accessing their privacy policies. The website also places privacy-related links in a 'Privacy Policy' section in its footer, though unlike the previous case (see section 6.1.1), the link is more prominent and easier to distinguish. Regardless, it still requires that the parent or guardian search the website for a link to the documents, which, as mentioned earlier, is not advised by COPPA specifically. On a related note, it was identified that Fitbit provides versions of both the main privacy policy and their children's privacy policy in several different languages and additionally has a rather straightforward and clear readability. For details on rights of data subject and user consent and permission, Fitbit presents substantial information to the recipient with a significant level of granularity, leaving little to no room for confusion or potential mismatch of statements.

There was cause for alarm when observed that the main Fitbit privacy policy fails to properly expand on how external tools are used and incorporated in their services. Despite a section dedicated to mentioning third party usage, unlike Garmin which includes a list of their third party assets, Fitbit does not provide useful information that would assure parents and guardians of what kind of external service will be processing their child's data. Both the GDPR and the California Consumer Privacy Act (CCPA)[4] determine that privacy policies must detail the usage of third party services by the product or application, and COPPA is emphatic about naming these third party operators along with their contact information and respective privacy policies.

> *Name each third party operator, such as an advertising network or social network plug-in, that collects or maintains children's personal information through your site or service. For each, include a name and contact information (address, telephone number, and email address). If more than one is collecting information, it's okay to give contact information for only one as long as that company will respond to all inquiries from parents about your site or service's practices. Even so, you still have to list all third parties in your privacy policy.*
> – **FTC - Complying with COPPA: Frequently Asked Questions**

Another potential issue observed was that neither privacy policy included any measures taken by the company to handle data security; a section titled 'Information Security' is available on the main privacy policy but offers no further information other than Fitbit affirming that they utilise Transport Layer Security (TLS) for encryption. There were also no further details available to properly reassure the parent or guardian of what happens if they decide to opt out of granting consent. On a positive note, Fitbit includes several instances of how they handle health-related data and what they can be used for, as defined in the Recital 35[5] of the GDPR.

[4] California Consumer Privacy Act (CCPA) <https://oag.ca.gov/privacy/ccpa>
[5] Recital 35 - Health Data - GDPR <https://gdpr-info.eu/recitals/no-35/>

There is also no indication of certifications for the products by any of the COPPA Safe Harbor enabled organisations in either privacy policy. Nevertheless, Fitbit appears to aim to ensure that changes in their current policies reach the parents and guardians through notifications sent directly to the latter, requiring that they are aware of these modifications and agree to them.

6.1.3 Privacy Policy Compliance

The elicited concerns previously suggest that there could be a correlation between what is not being explicitly included in these privacy policies and potential mishandling of personal data from children (or general users) behind the scenes. It is known that there is some degree of power exercise between these companies and the potential customers of their products (REBELO; VALENçA; LINS, 2021), meaning that parents and guardians still resort to purchasing products from these companies due to their respective reputations. However, it was observed throughout the initial phases of the research that products from smaller companies such as TickTalk 4 (see Appendix A.3.4) provide extensive and detailed information in their privacy policy, especially regarding their security practices to ensure data security.

Both companies assessed as part of the evaluation have a history of data breach cases reported in the media. In the case of Garmin, a 2020 ransomware hacker attack affected their systems and required a $10M fee to regain control of their services and put them back online[6]. In 2021, an unsecured database containing over 61 million records related to fitness trackers and wearables was responsible for exposing Apple and Fitbit users' data online[7].

Research shows that Fitbit is relatively successful among children (CREASER et al., 2021) and, as the adoption of this device to improve physical activity increases, there is greater concern when other factors are also considered. Google, the owner of Fitbit, was the on the receiving end of an enforcement action by the Federal Trade Commission (FTC) for COPPA violations in 2019 for collecting personal information from viewers of child-directed channels without obtaining parental consent or notifying parents, resulting on a $170M settlement[8]. Users are also able to create an account using single sign-on (SSO) options such as Google and Facebook, which have their own privacy related concerns. Studies demonstrate that when users grant services access to their data, they are not provided information on the duration of the access, which in turn poses ongoing danger to user privacy. Additionally, that user-friendly logins such as SSO are listed last, suggesting a dark pattern favouring options that release more user data (MORKONDA; CHIASSON; OORSCHOT, 2021).

[6]Garmin reportedly paid multimillion-dollar ransom after suffering cyberattack <https://www.theverge.com/2020/8/4/21353842/garmin-ransomware-attack-wearables-wastedlocker-evil-corp>

[7]Fitbit, Apple user data exposed in breach impacting 61M fitness tracker records <https://www.fiercehealthcare.com/digital-health/fitbit-apple-user-data-exposed-breach-impacting-61m-fitness-tracker-records>

[8]Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law>

7 Conclusion

7.1 Contributions

It is known that security and privacy related discussions have grown exponentially over the past few years, and certainly when the protection of minors' personal data takes centre stage. As the adoption of gadgets among children increases, parents and guardians, as well as researchers, find themselves preoccupied with how much information these devices and services can retain, and whether the companies responsible for them are properly handling such sensitive type of data. Through the quality assessment and audit process, presented as part of this work, it was possible to understand the granularity of information provided by companies to inform the user of these privacy and security related aspects, the level of transparency behind the available policies, and whether or not these privacy policies follow guidelines from established laws and regulations.

This study aimed to initially conduct an investigation of existing products targeted at children and their respective privacy policies to identify gaps related to information surrounding children's privacy and, based on these findings, understand how to redirect the attention to these gaps. Due to a lack of preoccupation with holding powerful companies accountable for failing to disclose their policies with a considerable level of detail, requirements established by privacy laws and regulations are often overlooked and untended to.

From a research perspective, the contribution of this study is centred on proposing a structured process to assess the quality metrics of children's privacy policies, aiming to understand the kind of information being disclosed to parents and guardians surrounding the data handling practices from these companies either prior or post purchase of their products. The main goal is to redirect the responsible entities for assembling these policies to resources that will guide them towards compliance and general good practices. Furthermore, an analysis of the results generated by the proposed audit process was conducted to evaluate the correlations between the compliance (or lack thereof) of these privacy policies with privacy regulations guidelines, and whether any conscious efforts to provide unclear information to parents and guardians in these policies were interpreted. Due to the knowledge that the evaluated companies hold power of reference over customers, the primary motivation behind the audit process proposition is to achieve some level of power balance between those creating these privacy policies and those accepting the policy terms.

From a practical perspective, the main contribution is centred in the proposed audit process. The secondary contributions are the artefacts for execution of the process, which are the developed quality criteria catalogue and audit questionnaire tool. These artefacts also have their

own capabilities and can be utilised independently. With the structured audit process format, however, irrespective of the evaluator responsible for performing the assessment, companies should be able to attain relevant metrics and feasible directives to remediate the observed gaps. Additionally, by providing a well-rounded set of policies to users – in this case, parents and guardians – the relationships between users and companies should be strengthened and future privacy-related issues prevented.

7.2 Limitations

- **No direct access to the evaluated companies**
  - Despite combining efforts to conduct a thorough assessment of the evaluated cases in Chapter 5, the results were interpreted internally and were not submitted to the respective companies to address each directive for correction. Therefore, regardless of the generated metrics and combined efforts to remediate the concerns, these results have not been cross-validated with the subject of the evaluation to move further along in the subsequent stages of the process.

7.3 Threats to Validity

- **Limited cases for analysis**
  - The results of the evaluation were attained by executing the process with a limited number of cases, which could lead to a spectrum of different interpretations from different researchers; the number of cases, however, was consciously determined to guarantee that other aspects, such as the exercise of power, could be simultaneously understood. Additionally, the chosen approach to analyse policies from a very specific realm of gadgets implies that wearables processing the type of sensitive information such as health data was prioritised.

7.4 Related Work

A relevant contribution regarding the display and usability of privacy policies can be found in the study by Angulo et al. where the approach of a user-friendly privacy policy was proposed for a project, observing that users responded well to the developed features and perceived the importance of being more aware of and concerned about their privacy. (ANGULO et al., 2012) Additionally, it was noted that there needs to be a recurrent effort to guarantee that privacy policies are more intuitive and as seamless as possible (ANGULO et al., 2012). Angulo's work was important to understand the perspective of the user and how the content of the policy should potentially be displayed in the most efficient way for better comprehension.

Regarding privacy concerns from a requirements perspective, the research by Peixoto et al. offers a broader understanding of how modelling languages actually address privacy-related concepts and the relationship between these concepts in a comprehensive catalogue (PEIXOTO et al., 2020). The results were relevant throughout this research as they provided a basis for understanding the extent to which these privacy requirements reflect on the way privacy policies are conceived and whether there is a correlation between the identified gaps identified in the evaluation phase (see Chapter 5).

The work by Terra et al. on assessing the privacy policies of applications proposes a catalogue of quality criteria to assist with a spectrum of concerns behind a well formulated privacy policy: the consistency between requirements and the content of the policies; writing concise documents; outlining data collection practices in a straightforward way; and lastly, guarantying that users are able to understand these policies (TERRA; VILELA; PEIXOTO, 2022). Our study was heavily inspired by the results generated by this original catalogue, leading to a reformulated version to accommodate a different perspective and later extended in the form of a questionnaire tool, while preserving the core categories originally outlined for the quality analysis.

To understand users' privacy concerns in the wearables realm, the study by Lidynia et al. showcases the importance of investigating security aspects around sensitive data and how these concerns are perceived by the users, understanding that these individuals find storage location and possible recipients of the collected data to play a significant role in adopting fitness trackers (LIDYNIA; BRAUNER; ZIEFLE, 2017). Similarly, the study by Gabriele et al. reinforces the idea that there should be a greater understanding of how fitness trackers handle security and the privacy of users' personal data, providing results that the adoption of these wearables require significant amount of awareness of data collection practices, ownership, storage, and sharing practices related to the tracking of said information (GABRIELE; CHIASSON, 2020).

Our research converges the concerns raised in these previous studies from a practical perspective by operationalising the evaluation of privacy policies. The redesigned quality catalogue centralises the concerns around the readability of privacy policies, additionally to the privacy and security matters. It serves as the backbone for the implemented audit questionnaire tool. The audit questionnaire tool provides constructive directives for privacy policy enhancement based on the laws and regulations the companies should comply with. The structured audit process, by including these artefacts, allows for a centralised and organised execution of the privacy policy evaluation.

7.5 Future Work

The following topics are proposed for future studies and extensions of the work presented in this research:

1. **Improvement of the audit questionnaire tool**

    - The quality audit questionnaire presented in Section 4.1.2 is a tool built to assist with a manual evaluation of privacy policies, hence it requires an evaluator to input the answers to generate results. To enhance the capabilities of the proposed questionnaire, the tool can benefit from incorporating machine learning techniques such as natural language processing (NPL) and data mining to automate the interpretation of the policies and generate an automatic report of both metrics and directives for the evaluator. Additional to the previously mentioned improvements, an extended incorporation of a Flesch Reading Ease calculation to generate readability scores and perform tests based on the Flesch-Kincaid grade level formulae to better assess this topic is proposed.

2. **Automate the audit process flow**

    - As an extension of the proposed improvement above, the second and third stages (see Sections 4.1.3.1 and 4.1.3.2) of the designed process flowchart (see Fig. 5) can be automated and include the reformulated questionnaire in the new implementation to further enhance the entire dynamics of the quality assessment. This enhancement could run the questionnaire automatically and generate the improvements and refinements based on the directives generated by the results from the assessment. This could assist the evaluator and the company to outline the next steps concerning the reformulation of the privacy policy.

3. **Evaluate different products**

    - As reiterated in a previous section (see section 7.2), this study focused primarily on evaluating a selected number of products from specific companies, meaning that the scope was purposefully small and therefore limited. In order to expand the analysis and garner more metrics surrounding the quality of different privacy policies from different products, a more extensive evaluation can take place, aiming to enlarge the scope and promote a greater discussion around the topic.

A Appendix

A.1 Data search queries

This appendix lists the queries used to collect the required data for this research as described in section 3.1.1 of chapter 3.

- connected devices
- data privacy
- privacy requirements
- security requirements
- fitness trackers AND privacy risks
- children AND fitness tracker AND privacy AND coppa
- children AND activity tracker AND privacy
- children AND wearables AND privacy
- children AND wearables AND privacy AND coppa

A.2 Children Wearables Reviews

A.2.1 Verizon GizmoWatch

The GizmoWatch is one of the connected devices offered by Verizon, an American telecommunications provider, described as specifically designed with children's safety in mind. This review encompasses a general evaluation of all GizmoWatch devices listed on Verizon's website: GizmoWatch 2, GizmoWatch 3, and GizmoWatch Disney Edition. Per the company's claim, the GizmoWatch presents features compatible with parents' expectations, such a GPS locator, reminders and easy-to-use parental controls with *"the goal of fostering independence to provide parents a little peace of mind"*[1], highlighting that those devices are restricted from installing any outside apps.

The smartwatches are connected via the GizmoHub[2] app on parents/guardian's smartphones to *"provide an easy way to keep up on [your] child's whereabouts"*[3], including features

[1] Verizon GizmoWatch 2 <https://www.verizon.com/connected-smartwatches/verizon-gizmowatch-2/>

[2] GizmoHub App <https://apps.apple.com/us/app/gizmohub/id921596283>; <https://play.google.com/store/apps/details?id=com.vzw.gizmopal&hl=en&gl=US>

[3] Verizon GizmoWatch 3 <https://www.verizon.com/connected-smartwatches/verizon-gizmo-watch-3/>

like step trackers for the encouragement of healthy habits (via lifestyle apps to enable movement fun with activity-tracking that has characters to motivate and reward children, like in the case of the Disney Edition[4] device) and to-do lists with rewarding capabilities. Additionally, parents can configure trusted contacts that kids can send voice notes to, call or text, powered by a cellular plan.

> *"Verizon sells this rather bare bones smartwatch/wrist phone alongside a cell service plan. The watch, targeted at the younger kid age-group who aren't quite old enough to have a phone of their own, lets parents and caregivers track kids with GPS location, set up a list of 10 trusted contacts that the child can call, set up reminders, track steps, and push to-do lists."* (MOZILLA, 2022e)

The technical privacy-related elements from GizmoWatch identified by Mozilla are described in the table below.

Can it snoop on me?		
Camera	**Microphone**	**Device**
Device: No *App: Yes*	*Device: No* *App: Yes*	*Device: Yes* *App: Yes*
What can be used to sign up?		
Email	**Phone**	**Third-party account**
Yes	*No*	*Yes*
What data does the company collect?		
Personal	**Body related**	**Social**
Your name, mobile telephone number, email address; and your child's name, age and gender; precise geolocation	*N/A*	*Trusted contacts*

(MOZILLA, 2022e)

Mozilla also claims that the GizmoWatch checks all boxes for all five criteria in their Minimum Security Standards[5].

- **Encryption:** *Yes*
- **Strong password:** *Yes*
- **Security updates:** *Yes*

[4] Verizon GizmoWatch Disney Edition <https://www.verizon.com/connected-smartwatches/verizon-gizmowatch-disney-edition/>

[5] Minimum Security Standards - About our Methodology <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/>

- **Manages vulnerabilities:** *Yes*[6]
- **Privacy policy:** *Yes*

The main concern regarding this product for Mozilla stems from the fact that Verizon seemingly does not have the most reputable track record when it comes to protecting their user's privacy. Several reports in the media regarding Verizon's practices came to light over the past five years. In 2017, a significant batch including 6 million customers' account information was exposed[7]. In 2018, Wired reported that the FCC fined several companies for selling users' location data and Verizon was among the list [8]. Again in 2020, the FCC fined Verizon directly in over $48M over location data violations based on several media reports from previous years[9].

> *"So, when they offer up a Gizmowatch and GizmoHub app for kids that can track them using GPS, uses cellular data to send calls, voice and text messages, as well as track steps and more, we admit, we were skeptical. Why would anyone want to let a company with such a history of privacy violations and bad acting track their young child?"* (MOZILLA, 2022e)

Similarly, the review also raises awareness to the possibility of Verizon selling data per the definition of 'sale' in California Consumer Privacy Act (CCPA) with the combination of users' data and personal data obtained from third parties. Due to a confusing list of privacy policies, Mozilla claims, these policies indicate that Verizon can collect a significant amount of personal information and data data from the user (child and parent/guardian) and it is unclear how the data is handled; both CPPA and the Children's Online Privacy Protection Rule (COPPA) have restrictions regarding the sharing and selling of information from individuals under the age of 16; for children under the age of 13, permission must be opt-in coming from parents/guardians. Mozilla also reports that it seems unclear children's data can always be deleted from Verizon's services (MOZILLA, 2022e).

A.2.2 Spacetalk Adventurer

The Spacetalk Adventurer 4G Kids is a connected smartwatch with cellular and GPS tacking capabilities from Spacetalk, an American company that describes itself as *"the global*

[6]See a security vulnerability? Say something - Verizon <https://www.verizon.com/solutions-and-services/report-security-vulnerability/>

[7]Verizon Breach: 6 Million Customer Accounts Exposed <https://www.bankinfosecurity.com/verizon-breach-6-million-customer-accounts-exposed-a-10107>

[8]The FCC Fines Wireless Companies for Selling Users' Location Data <https://www.wired.com/story/fcc-fines-wireless-companies-selling-users-location-data/>

[9]FCC Proposes $48.3M Fine against Verizon in Location Information Case <https://www.fcc.gov/document/fcc-proposes-483m-fine-against-verizon-location-information-case>. A 2021 report by The Verge also brought to light that Verizon could be potentially demanding access from users to access browsing history even after they have opted-out[10]

leader in children's safety wearable communication devices"[11]. The product is said to be designed for granting children more freedom and parents greater peace of mind, targeted for kids aged 5 - 12. The Adventurer watch allows family members to call and text the child combined with other safety features like SOS alerts, Safe Zones, Safe contact lists and GPS locations; additionally, they highlight no open access to the internet or social media.

Some additional features listed by Spacetalk include being able to connect to your child's device with the Spacetalk[12] app for controlling and managing features the child can use; a School Mode that limits features on the device during school hours to prevent distraction; step counter and heart rate monitor to encourage children to be active; alarms and reminders to assist children with staying organised.

> *"Parents can use the app to set up safe zones where kids can go and safe contact lists of people they can call or receive calls from. Yay for being able to keep close tabs on your kids. Boo for teaching kids that this sort of all day, everywhere surveillance is a normal, good thing."* (MOZILLA, 2022c)

The technical privacy-related elements from Spacetalk Adventurer identified by Mozilla are described in the table below.

Can it snoop on me?		
Camera	**Microphone**	**Device**
Device: Yes *App: Yes*	*Device: Yes* *App: Yes*	*Device: Yes* *App: Yes*
What can be used to sign up?		
Email	**Phone**	**Third-party account**
Yes	*No*	*No*
What data does the company collect?		
Personal	**Body related**	**Social**
First name, last name, date of birth, gender, username (similar identifier), billing address, email address and telephone numbers, location data.	*Weight, average activity levels, movement/physical ability, medical conditions, medication/prescriptions*	*N/A*

(MOZILLA, 2022c)

Mozilla also reports that the Spacetalk Adventurer checks all boxes for all five criteria in their Minimum Security Standards[13].

[11] Spacetalk Watch - Spacetalk <https://us.spacetalkwatch.com/>

[12] Spacetalk App <https://apps.apple.com/au/app/spacetalk/id1273641588> <https://play.google.com/store/apps/details?id=com.mgmwireless.allmytribe3&hl=en&gl=US>

[13] Minimum Security Standards - About our Methodology <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/>

- **Encryption:** *Yes*
- **Strong password:** *Yes*
- **Security updates:** *Yes*
- **Manages vulnerabilities:** *Yes*[14]
- **Privacy policy:** *Yes*

Somewhat similar to what was observed for the GizmoWatch (see **??**), Mozilla highlights that there are incongruities in Spacetalk's handling of personal data and the possibility of Verizon selling data per the definition of 'sale' in California Consumer Privacy Act (CCPA) with the combination of users' data and personal data obtained from third parties. These policies indicate that Spacetalk can too collect a lot of personal information and data from the user (child and parent/guardian) and it is unclear how the data is handled. Mozilla also reports that it is not guaranteed that children's data can always be deleted from Spacetalk's services, and in some cases, the request for deletion will not be granted (MOZILLA, 2022c). Although Spacetalk does not have any media reports suggesting violation of user's data, the review reiterates that the privacy information provided by the company is not user-friendly and, as previously mentioned, generally unclear.

> *"Nowhere in their privacy policy do they say they don't sell their users data (...) They also say they do use some of that data for marketing and personalization purposes and that they share some tracking data with third parties for advertising purposes."* (MOZILLA, 2022c)

Lastly, the review alerts that, Spacetalk states in their privacy policy that they can collect personal information from third parties such as advertising networks and social media platforms and use it for purposes service as well as potentially marketing and customisation. However, they also add in that the company can use personal information for vague purposes by claiming the purposes extend to their own Privacy Policy "or other policy" (MOZILLA, 2022c).

A.2.3 TickTalk 4

The TickTalk 4 is the smartwatch developed by the American company TickTalk that is said to have been designed by parents for children ages 5-12 with no internet, social media or gaming capabilities. Similar to the previous two devices, TickTalk 4 is cellular powered for allowing parents to call their children, video chat, send photos, text messages and track their

[14] See a security vulnerability? Say something - Verizon <https://www.verizon.com/solutions-and-services/report-security-vulnerability/>

location. Additionally, the company affirms that their goal *"has always been to keep you connected to your child and give you a way to make sure your child is safe when they're away from home"*[15]. The device grants parents the ability to set Emergency SOS contacts, block unknown numbers, approve contacts, view call logs and SMS text requests. For connectivity, the smartwatch must be paired with a compatible smartphone carrying the TickTalk app[16]. Among its features, there are: an activity tracker with daily step goals to encourage an active lifestyle and compete with friends to earn the gold, silver, or bronze medals; 50+ pre-programmed reminders and customizable alert; free, unlimited streaming of kid-friendly songs, podcasts and stories.

The technical privacy-related elements from TickTalk 4 identified by Mozilla are described in the table below.

Can it snoop on me?		
Camera	**Microphone**	**Device**
Device: Yes *App: Yes*	*Device: Yes* *App: Yes*	*Device: Yes* *App: Yes*
What can be used to sign up?		
Email	**Phone**	**Third-party account**
Yes	*Yes*	*Can't Determine*
What data does the company collect?		
Personal	**Body related**	**Social**
Child's Name, Birth date, gender; *Parent's Name,* *Profile Picture and/or Avatar,* *Phone Number,* *Birth Date (Optional),* *Gender (Optional),* *Precise Location,* *Past Precise Locations* *(if History Route is enabled).*	*N/A*	*N/A*

(MOZILLA, 2022d)

Mozilla also claims that the TickTalk 4 does not check all boxes for all five criteria in their Minimum Security Standards[17].

- **Encryption:** *Yes*

[15] TickTalk 4 Kids Smartwatch <https://www.myticktalk.com/>

[16] TickTalk Kids Smartwatch <https://apps.apple.com/us/app/ticktalk-kids-smartwatch/id1444054034>, <https://play.google.com/store/apps/details?id=com.xdreamllc.ticktalk3&hl=en&gl=US>

[17] Minimum Security Standards - About our Methodology <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/>

- **Strong password:** *Yes*
- **Security updates:** *Yes*
- **Manages vulnerabilities:** Can't determine
- **Privacy policy:** *Yes*

Mozilla highlights early in the review that TickTalk faced backlash with Children's Advertising Review Unit (CARU)[18], which operates under the BBB National Programs[19] as a watchdog organisation, for violating COPPA requirements. The statement discloses that TickTalk *"failed to provide clear and complete, and non-confusing, notice of its children's information collection practices in its privacy policy and failed to provide any notice that would constitute a direct notice to parents as required by COPPA"*[20]. Furthermore, CARU also claims that TickTalk failed at displaying the product and app's privacy policy in a prominent location prior to purchase, determining that *"the site fails to prominently lay out for parents, in an easy-to-find location prior to purchase, specifically what personal information TickTalk can collect from children (actively or passively) and how it uses and/or discloses such information"*.

On a similar note, like the GizmoWatch and Spacetalk Adventurer, both Mozilla and CARU report that TickTalk presents users with an ambiguous set of policies, terms of service, and other online statements included inconsistent, confusing and/or contradictory statements about its collection, use, or disclosure of children's personal information"[21] (MOZILLA, 2022d). Moreover, the report reiterates that the company did not provide means for parents to provide verifiable consent to its information collection practices prior to the collection of information from children.

> *"This smart tracking watch for kids really does highlight the issue of privacy versus safety and how those two conflict. So, hows does the TickTalk watch do when it comes to protecting you and your kids' privacy?"* (MOZILLA, 2022d)

The same report also discloses that an agreement between CARU and TickTalk was settled once the review unit presented the company with corrective actions and TickTalk willingly participated in CARU's self-regulatory program, then further presented a detailed plan to remedy the concerns raised in the decision to comply with COPPA and CARU's Privacy Guidelines20.

[18] Children's Advertising Review Unit (CARU) <https://caru.bbbprograms.org/>

[19] *BBB National Programs is a non-profit organization creates a fairer playing field for businesses and a better experience for consumers through the development and delivery of effective third-party accountability and dispute resolution programs.*

[20] Children's Advertising Review Unit Finds TickTalk Tech in Violation of COPPA and CARU's Privacy Guidelines; Company Agrees to Corrective Actions <https://bbbprograms.org/media-center/dd/ticktalk-tech-coppa-caru-privacy-guidelines-violation>

[21] 20

Nevertheless, the review once again raises concern over the possibility of TickTalk potentially selling data per the definition of 'sale' in California Consumer Privacy Act (CCPA) by combining users' data and personal data obtained from third parties, which categorises as a CPPA and the Children's Online Privacy Protection Rule (COPPA) violation based on their restrictions regarding the sharing and selling of information from individuals under the age of 16; for children under the age of 13, permission must be opt-in coming from parents/guardians (MOZILLA, 2022d).

A.2.4 Huawei Watch Kids 4 Pro

The Huawei Watch Kids 4 Pro is a smartwatch developed by the Chinese technology company Huawei with cellular and network capabilities for stable voice calls and SMS5 thanks to the full 4G VoLTE6 coverage. The device allows parents/guardians to track children's locations with fast, with pin-point accuracy supported via GPS, Beidou, GLONASS, A-GPS,WLAN positioning, base station positioning, roaming positioning, accelerometer-assisted positioning, and SOS camera assisted positioning [22]. This smartwatch also includes several activity tracking and healthy lifestyle capabilities, such as Swim Training Mode with different swim styles; sports and activity tracking modes like skipping rope and sit ups. Unlike the devices previously, the Huawei Watch Kids 4 Pro was the only one who does not specify internet access restrictions..

> *"Want to track your kids everywhere in every way? I mean, really track them? This kids-focused smartwatch is for you. Call your kids with either voice or HD video right from their wrist, track them anywhere with what Huawei calls, "9-system AI positioning," get notifications if you kid leaves a "safe area" you set up, even track how many hours your kid spends outside in the sun."* (MOZILLA, 2022b)

The technical privacy-related elements from Huawei Watch Kids Pro 4 identified by Mozilla are described in the table below.

Can it snoop on me?		
Camera	**Microphone**	**Device**
Device: Yes *App: No*	*Device: Yes* *App: No*	*Device: Yes* *App: Yes*
What can be used to sign up?		
Email	**Phone**	**Third-party account**
Yes	*Yes*	*No*
What data does the company collect?		
Personal	**Body related**	**Social**

[22] HUAWEI WATCH KIDS 4 Pro <https://consumer.huawei.com/en/wearables/k4-pro/>

Child's date of birth, HUAWEI ID (mobile number/email address), nickname	*N/A*	*N/A*

(MOZILLA, 2022b)

Mozilla also claims that the Huawei Watch Kids 4 Pro does check all boxes for all five criteria in their Minimum Security Standards[23].

- **Encryption:** *Yes*
- **Strong password:** *Yes*
- **Security updates:** *Yes*
- **Manages vulnerabilities:** *Yes*[24][25]
- **Privacy policy:** *Yes*

Once again, the review brings concerns related to privacy and the mishandling of data on Huawei's end. According to Mozilla, *"this smart watch for kids does not seem good for privacy at all; it currently receives all the privacy dings we can give it"* (MOZILLA, 2022b), highlighting that Huawei does not specify the purposes and recipients for sharing children's personal data. Similar to the previous devices, Huawei provides an incoherent and difficult-to-read list of policies in their privacy protection statements, where Mozilla identified that even though the company claims to "automatically disable personalized ads and direct marketing features and provide content that is appropriate for children when use by a child is detected", it also collects and uses other personal information of the child for broad and vague purposes outlined in the privacy policy (MOZILLA, 2022b). Mozilla also points to the fact that Huawei delegates responsibility to children for redirecting parents/guardians to reading privacy policies.

> *"Children must ask their guardians to carefully read this Statement and seek permission or guidance from their guardians before using our products or services or providing information to us."*[26]

[23] Minimum Security Standards - About our Methodology <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/>

[24] Huawei PSIRT <https://www.huawei.com/en/psirt>

[25] Huawei | Vulnerability Disclosure Policy | HackerOne <https://hackerone.com/huawei?type=team>

[26] Huawei Consumer Business Statement About Children's Privacy Protection <https://consumer.huawei.com/minisite/legal/childprivacy/statement.htm?code=CN&language=en-GB>

Lastly, Mozilla notes that these concerns are magnified by the fact that Huawei does not have the most pristine track record. In 2019, The Washington Post investigated leaked documentation that exposed Huawei's secret operations in building wireless networks in North Korea[27]; In 2020, it was also reported that Huawei tested heavily-based AI software with aim to identify and suppress minorities in China[28], forcing the company to issue a statement on their official website to reiterate commitment with human rights[29]. Additionally, Huawei also released a security advisory statement regarding leak vulnerability in some of its products[30].

A.3 Wearables Privacy Policy Quality Assessment

A.3.1 Overview

The following results were generated from performing an assessment with the catalogue proposed by Terra et al. (see B.1) to gauge quality in the privacy policies from each device presented in the preceding section. Note that, although the original catalogue is mainly focused on applications, the responses were elaborated based on a product perspective due to the nature of this study. To assess accessibility aspects, the ayy1 Color Constrast Accessibility Validator[31] was used for colour contrast validation; for readability aspects, the WebFX Readability Test[32] was used for readability indicators.

A.3.2 Verizon GizmoWatch

For the category of **User Experience**, it was observed that Verizon does not provide straightforward ways for the user to easily access their privacy policies. On the Gizmo page, there is no mention of a product-specific privacy policy nor any links for the user to read any other provided policies; the only instance of a privacy policy can only be found at the footer of the website page. However, both the Gizmo and the Verizon privacy policy pages are responsive and provide an even experience for those with low vision and other disabilities.

- **Does the application present the Privacy Policy when the user accesses the platform?**

[27] Leaked documents reveal Huawei's secret operations to build North Korea's wireless network<https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html>

[28] Huawei tested AI software that could recognize Uighur minorities and alert police, report says <https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/>

[29] HUAWEI'S COMMITMENT TO HUMAN RIGHTS 2020 <https://www.huawei.com/uk/declarations/huawei%20human%20rights%20commitment>

[30] Security Advisory - Information Leak Vulnerability in Some Huawei Product <https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200108-01-phone-en>

[31] Color Contrast Accessibility Validator (WCAG 2.1 AA SC 1.4.3 Test for Color Contrast) <https://color.a11y.com/>

[32] WebFX Readability Test <https://www.webfx.com/tools/read-able/>

The Privacy Policy can only be found at the footer of the Verizon website, which then redirects the user to a general privacy policy page that includes app and service specific policies. There are no links to be found on the main product page for both the Gizmo Privacy Policy nor Verizon's Privacy Policy; only a California Proposition 65 warning is provided.

- **How easy is it for the user to find the Privacy Policy in the App?** Hard. The link to the privacy policy can only be found in the footer of the website.
- **Is the document adequately translated to all the languages that the application supports?** Yes, considering that Verizon operates solely in the United States. Both English and Spanish versions are available.
- **Is the Privacy Policy accessible to people with disabilities (PWD)?** The website presented no issues related to colour contrast. No additional accessibility tools are provided on the privacy policy page.
- **Does the document present a readability level compatible with what the application users can read?** The readability score for both the Gizmo and the Verizon privacy policy suggest that individuals aged 14-15 should easily understand the text, meaning parents/guardians should be able to comprehend it.
- **Is the document responsive?** Yes, the document is responsive.

The category of **Privacy Policy Content** brings to light that Verizon provides very minimal information to the user regarding its data practices. There is no expanding into specific details, especially in regards to children, despite having a privacy policy aimed at outlining children-related policies. Furthermore, it affirms that *"Gizmo's privacy practices are covered by Verizon's Privacy Policy as well as the practices described here"* (VERIZON, 2023a), potentially aggravating users' confusion and causing a spectrum of mismatching information. Despite claiming that *"in the event of a conflict between the two policies, the practices described in this policy govern when you are using Gizmo products and services"* (VERIZON, 2023a), it further suggests that there could be underlying uninformed practices.

- **Is the Privacy Policy based on the assumption that the visit to the application implies the user's consent to the Policy, independent of the user reading the document or not?** Could not determine it.
- **Does the policy specify clearly what data is collected?** Yes. Users are able to find a section with a comprehensive list of information that is collected.

Information we collect from you.

We collect information when you set up Gizmo services through the GizmoHub app, including your name, mobile telephone number, email address, and your child's name, age, photo, and relationship to you. Additional information that is collected depends on the Gizmo products your child uses and the features that you choose to activate. If you activate a Gizmo wearable, we collect information through the GizmoHub app about trusted contacts and buddies you assign, audio and video call and messaging usage between you and your child and messages you send to your child.

Information we collect from trusted contacts.
We collect information from your trusted contacts through the GizmoHub app including email address, mobile telephone number, audio and video call and messaging usage between the trusted contact and your child, and messages sent by trusted contacts to your child.

Information we collect from your child (including children under 13).
When your child uses a Gizmo wearable, we collect device information (such as identifiers, mobile telephone number, operating system, and watch version), app and feature usage, location, audio call usage, and wireless network data usage. (...) we also collect messaging usage, the number of steps taken, and text messages exchanged between your child and you and between your child and your trusted contacts and buddies. (...) also collect audio messages exchanged between your child and you and between your child and your trusted contacts or buddies. (...) we also collect video calling usage as well as photo and video messages exchanged between your child and you, and between your child and your trusted contacts which include other Gizmo device users and buddies if you add them as trusted contacts. (VERIZON, 2023a)

- **Does the Privacy Policy specify clearly how the data is collected?** No.
- **Does the Privacy Policy clearly specify if the application does use some tool or external service?** The only mention of external service used by the GizmoWatch on the privacy policy is regarding weather-related services.

  Approximate geolocation identifying an area of approximately ⅔ of a mile radius of your child may also be used by our partner Accuweather to provide weather updates if requested by GizmoWatch Disney Edition, GizmoWatch 2, and GizmoWatch 3 users. (VERIZON, 2023a)
- **Does the Privacy Policy specify how the company can use the collected data?** Verizon only vaguely mentions the purposes for data collection and does not expand on the topic on the Gizmo privacy policy.

We use the information we collect to deliver, maintain, support and improve Gizmo services, including to provide you with location information for your Gizmo devices, and for analytics. We share personal information with vendors who work on our behalf. These vendors are contractually obligated to use personal information shared with them solely to help us provide Gizmo services and not for advertising, profile creation, or any other purpose. We do not sell, share or use your or your child's information for any other purposes.(VERIZON, 2023a)

However, on the full privacy policy, a number of other purposes are listed, implying that Verizon will also utilise user data to *deliver and maintain products and services; establish and maintain your account and billing records; measure credit and payment risk; provide account-related services and information; help you with service and technical support issues or questions; manage and protect our networks, services, employees and users; detect and prevent fraud; help us improve and personalize your servicesl research, develop and market new products and services; authenticate you; determine your eligibility for new products and services; better predict content and marketing offers that may interest you; deliver personalized content and offers to you.* (VERIZON, 2023b)

- **Does the Privacy Policy specify whether the information can be shared or sold to third parties?** There are mismatches between Verizon's Privacy Policy and Gizmo's Privacy Policy. Due to the lack of straightforward practices, it could be implied that Verizon could be potentially selling combined users' data with information collected from third parties, which falls under the 'sale' definition proposed by the California Consumer Protection Act (CCPA) and could be infringing COPPA standards.

  "We share personal information with service providers who work on our behalf. These service providers are contractually obligated to use personal information shared with them solely to help us provide Gizmo services and not for behavioral advertising, to compile profiles, or any other purpose." (VERIZON, 2023a)

  "We allow third-party advertising companies to collect information about your activity on our websites and in our apps, for example through cookies and similar technologies, mobile ad identifiers, pixels, web beacons and social network plugins. These ad entities use information they collect to help us provide more relevant Verizon advertisements and other advertising purposes. This activity may be considered a sale under the CCPA."

  "You have a right to inform us that you do not want your personal information sold or shared. California law defines "sale or sharing" broadly to include sharing personal information for monetary or other valuable consideration and the sharing of your information for cross contextual advertising purposes, but the definition does not cover all

sharing of personal information. We do not knowingly sell or share personal information related to children under 16 years of age." (VERIZON, 2023b)

- **Does the Privacy Policy specify whether the data supply requested is voluntary or mandatory and the consequences of refusing to provide the requested information?** In the Gizmo privacy policy, Verizon provides a list of requirements for activating services provided by the device.

  "For Gizmo services to work, you must provide consent through the GizmoHub app for us to collect information from your child, as well as your and your child's location. Your precise location, your child's precise location, and other information collected about your child is "sensitive personal information" under some state laws. Your consent is required for us to collect, use and disclose such information, and we will not do so without your consent. Specifically, parents are asked to provide consent for all Gizmo devices that are paired with the app to collect device identifiers and phone information such as mobile telephone number, operating system, and watch version; location; steps taken; call, messaging and data usage; as well as photo, video, audio and text messages sent between the wearable and the GizmoHub app. You may revoke your consent at any time, however, certain Gizmo services will not be available without your consent. You may review the information collected from Gizmo devices. To revoke consent or request to review information, please contact us by email, telephone or mail at the address listed below." (VERIZON, 2023a)

- **Does the privacy policy specify the measures adopted by the application to ensure the confidentiality, integrity, and quality of Dice?** No.

- **Does the privacy policy specify how data is stored?** No.

- **Does the privacy policy mentioned agree with current law?** The Gizmo Privacy Policy redirects the user to the main Verizon Privacy Policy, where it states the following state laws: California Consumer Privacy Act, Maine Broadband Customer Privacy Rights, Nevada Privacy Rights, and the Virginia Consumer Data Protection Act. It also states that Verizon is a participant in good standing of the Children's Advertising Review Unit's (CARU) COPPA Safe Harbor Program despite only supposedly applying to two of their products, with no other mentions of COPPA throughout the entire policy page.

  "Verizon is a valid licensee, and participating member in good standing, of the Children's Advertising Review Unit's ("CARU") COPPA Safe Harbor Program ("CARU Safe Harbor") only with respect to the GizmoWatch Mickey Mouse 90th Anniversary Edition and the GizmoWatch Disney Edition. CARU conducts independent audits of these Services and uses other enforcement and accountability mechanisms in its certification process.

Services bearing the CARU Safe Harbor icon meet established online information collection, use, and disclosure practices in compliance with applicable privacy laws and best practices. Verizon's other Gizmo products follow the same guidance." (VERIZON, 2023a)

- **Does the policy mention access for minors' deity?** The app is targeted at parents and guardians over 18 years of age.
- **Does the policy address privacy issues related to children?** The Gizmo Privacy Policy loosely covers children's privacy rights.
- **Does the policy clearly explain what happens to the user's data if he deletes the account?** Verizon states that the company will *"retain account information as long as your Gizmo account is active in the GizmoHub app. We retain activity logs for up to 60 days from when you close your account."* (VERIZON, 2023a)

For the category of **Rights of the Data Subject**, the company provides enough information to the user in regards of their rights under state laws and more than one way to contact Verizon to handle product matters.

- **Is the user free to access data about yourself even stored by application?** Could not determine.
- **Does the privacy policy specify the user rights?** All information regarding state privacy laws can be found on the main Verizon Privacy Policy page.
- **Does the privacy policy report data to contact the company?** There are two separate contacts provided by Verizon.

  For more information or assistance, you can contact us by email at gizmopalsupport@verizonwireless.com, by phone at 800-922-0204, or at their local office. (VERIZON, 2023a)
  On the Verizon privacy policy: *privacyoffice@verizon.com or at their local office.* (VERIZON, 2023b)

When it comes to **Changes to the Privacy Policy**, Verizon explicitly states that it expects the user to check their privacy policy for any presented changes, failing to mention any other measures taken to assure that the changes reach the user.

- **How are changes in policies handled?** Verizon claims in their main privacy policy that users should check their privacy policy periodically for changes.

We may make changes to this privacy policy, so please check back periodically. You will be able to see that we made changes by checking the effective date below. You can also read about recent changes. (VERIZON, 2023b)

There is no such disclaimer in the Gizmo Privacy Policy, which could potentially lead to confusion and mismatching information. Furthermore, Verizon says the app-specific Privacy Policy governs over the main one as users are using those applications and services.

"In the event of a conflict between the two policies, the practices described in this policy govern when you are using Gizmo products and services." (VERIZON, 2023a)

- **What effect a change of privacy policy to an application imposes on the user?** The main Verizon privacy policy claims that if it chooses to *use or disclose information that identifies you personally in a way that is materially different from what we stated in our privacy policy at the time we collected that information from you, we will give you a choice about the new use or disclosure by appropriate means, which may include an opportunity to opt-out.* (VERIZON, 2023b)
- **How is the frequency of modification of the policy privacy?** There are two policy changes in the year 2022 with a six-month gap in between, followed by a change in June 2023. The Gizmo privacy policy does not have a version history other than the last recent change (June 2023).

The aspects of the **User Consent and Permission** category were covered based on the information provided by the privacy policy alone as we did not assess the application for the device.

- **What is the method of choosing the user for consent or not with the policy of privacy?** Could not determine.
- **Does the user have the option of not agreeing with the applicable privacy policy?** Yes (see 'Privacy Policy Content' section).
- **Is the user allowed to select what information it allows to be collected?** Could not determine.

A.3.3 Spacetalk Adventurer

For the **User Experience** category, it was noted that Spacetalk does not provide straightforward ways for the user to easily access their privacy policies. On the Spacetalk Adventurer page, there is no mention of a product-specific privacy policy nor any links for the user to read

any other provided policies. The user has to also manually search for the privacy policy via the built-in search engine on the website. Additionally, Spacetalk provides two separate privacy policies, though there is no reference to a Children's Privacy Policy anywhere on the main privacy policy. Nevertheless, both privacy policy pages are responsive and provide an even experience for those with low vision and other disabilities.

- **Does the application present the Privacy Policy when the user accesses the platform?** There are no links to the Privacy Policy anywhere on the main product page.
- **How easy is it for the user to find the Privacy Policy in the App?** Hard. The main product page has no links to its specific Privacy Policy and the Children's Privacy Policy can only be found by manually searching for it on the built-in Search engine within the website. The main Privacy Policy also does not have any links to the Children's Privacy Policy.
- **Is the document adequately translated to all the languages that the application supports?** The Privacy Policy is only available in English.
- **Is the Privacy Policy accessible to people with disabilities (PWD)?** The website presented no issues related to colour contrast. No additional accessibility tools are provided on the privacy policy page.
- **Does the document present a readability level compatible with what the application users can read?** The readability score for the main Spacetalk privacy policy suggests that that individuals aged 16-17 should easily understand the text; for the Spacetalk Children's privacy policy, the score suggests individuals aged 14-15 should understand the text. In both cases, parents/guardians should be able to comprehend it.
- **Is the document responsive?** Yes, the document is responsive.

The category of **Privacy Policy Content** reveals that Spacetalk actually provides a good amount of information to the user regarding their practices and the elements involved in how data is processed, albeit hard to comprehend and oftentimes contradicting. Similar to the Gizmo privacy policy (see A.3.2), the Spacetalk policies regarding children's privacy fails to elaborate further on how children's user data is handled de facto by providing a rather summarised overview of these policies. By not linking the two existing policies or describing whether they are complementary or not, it could potentially cause further confusion.

- **Is the Privacy Policy based on the assumption that the visit to the application implies the user's consent to the Policy, independent of the user reading the document or not?** Could not determine.

- **Does the policy specify clearly what data is collected?** Yes. Users are able to find a section with a comprehensive list of information that is collected. On the Children's privacy policy, however, the policies are rather vague and significantly less granular.

  What Personal Information We Collect, Hold and Use
  Personal information we may collect and hold includes:
  1. Personal Identifiers: first name, last name, date of birth, gender, username, or similar identifier and title, persistent online identifiers;
  2. Contact Data: billing address, email address and telephone numbers;
  3. Third-Party Contact Data: name (or nickname), phone number and photo (optional);
  4. Financial Data: payment card details;
  5. Transaction Data: details about payments to and from you and other details of products and services you have purchased from us;
  6. Usage Data: information about how you use our website and mobile app and fall reporting (time and velocity of fall events;
  7. Device Data: Phone Number, IMSI, Device ID, network information, request logs and Chat Handles, internet protocol (IP) address, internet service provider (ISP), browser type and version, operating system, time zone setting and location, device type and ID, date/time stamp, location data, and other technical information from the devices you use to access our website or mobile app;
  8. Profile Data: username, password, security pin and preferences;
  9. Audio and Visual Data: call recordings and pictures (optional);
  10. Location Data: Geographical location data and safe zone parameters;
  11. Health Information: weight, average activity levels, movement/physical ability, medical conditions, medication/prescriptions. (SPACETALKUS, 2021b)

  Information We Collect From Children and How We Use It
  When you set up a SpacetalkTM Watch for your child, we collect certain information from your child's device. This data is required to deliver the core features of the SpacetalkTM Watch and App and includes safe contact lists, safe zones based on the location of the watch wearer, geolocation, steps, calls, text messages, and photos (optional). We use the information collected to provide the Spacetalk services requested and to comply with our legal obligations. (SPACETALKUS, 2021a)

- **Does the Privacy Policy specify clearly how the data is collected?** Yes. Spacetalk lists several sources they utilise for collecting users' data on the main privacy policy. On the Children's privacy policy, it only states that the data is collected from the child's device (SPACETALKUS, 2021a).

  How We Collect Your Personal Information

We may collect Personal information from a variety of sources and methods.

Information You Voluntarily Provide
We will generally collect the above personal information from you directly. We collect personal information from you in various ways such as when you communicate with us, when you fill in an application or form or survey, if you apply for a job with us, if we provide a product or service to you, or when you participate in any of our activities. We may also retain any messages you send through the service. We may also retain fall reporting (time and velocity of fall events). We use this information to operate, maintain, and provide to you the features and functionality of the Services. We may also use this information to correspond with you, and to address any issues you raise about the Services.

Information We Collect When You Use Our Services
We may also collect data and personal information about individual from third parties and automatically, including through Web Servers and Location Data (as further set out below):

- Website Servers: When you access our website and online services the Web Server Data listed above is collected. We advise Google Analytics Demographic and Interest reporting may be used to develop specific offers or advertising from time to time.
- Location Data: we may collect this data in a variety of ways, including: Global Positioning System (GPS); Nearby Wi-Fi networks; Mobile cell tower triangulation; Near Field Communication; RFID.

Information We Collect From Third Parties
We collect personal information from other sources including our trusted partnerships with service providers and where we operate accounts email platforms, advertising networks, and social media platforms. We may also receive personal information from retailers in connection customer service inquiries. The collection, use, and disclosure of personal information received from third parties is governed by the third parties' privacy policies. Please carefully review these third-party privacy policies to understand how your information may be collected, used, and disclosed by these third parties.
(SPACETALKUS, 2021b)

- **Does the Privacy Policy clearly specify if the application does use some tool or external service?** Yes. Both privacy policies provide enough information to the user regarding third parties involved in their service provision.

Internal Third Parties
Because Spacetalk is part of a global business and group of companies, information may

be shared with our parent, subsidiaries and affiliated entities. Information will be treated confidentially and only disclosed on a need to know basis.

Service Providers
We work with other companies that help us provide our Services to our customers, and we may provide data to these companies for the purpose of providing the services and products to you and to facilitate our interests as stated above. Those service providers will only be provided with access to your information as is reasonably necessary for the purpose that we have engaged the service provider, and we will require that such third parties comply with our standards. (SPACETALKUS, 2021b)

When Information is Available to Others
We may share information with our service providers if necessary for them to support our "internal operations" (as defined by COPPA), including activities necessary for the site or service to maintain or analyze its functioning; perform network communications; authenticate users or personalize content; protect the security or integrity of the user, website, or online service; ensure legal or regulatory compliance; or fulfill a request of a child as permitted under COPPA. (SPACETALKUS, 2021a)

- **Does the Privacy Policy specify how the company can use the collected data?** Yes. Although the main privacy policy expands in great detail over what the user data can be used for, the Children's privacy policy lacks any mention of such topic. Moreover, it also states that the data could be used for purposes described in their policies as well as any other policy, potentially causing further confusion for the user.

  The Purposes for Which We Collect, Hold, Use and Disclose Personal Information
  We collect personal information which is reasonably necessary for one or more of our functions as noted above and including to:
  - maintain your account and contact details;
  - allow you to download and purchase our products and services'
  - process transactions and end user related information, including confirmations and invoices;
  - communicate with you;
  - provide you with access to protected areas of the site;
  - verify data for accuracy or completeness;
  - improve the quality of our services and develop new ones;
  - help our services deliver more useful, customized content such as location tracking and children's reward programs;
  - keep you posted on software updates, technical updates, security alerts and support and administrative messages;

- send marketing communication to you;
- conduct surveys to determine use and satisfaction;
- detect, investigate and prevent potentially unlawful acts or omissions or acts or omissions with the potential to breach our Privacy Policy or any other policy;
- comply with our legal obligations; combine or aggregate your personal information with data we collect from third parties and use it for the purposes set out in this Privacy Policy;
- protect a person's rights, property or safety; credit reporting purposes;
- as necessary to comply with legal requirements, to prevent fraud, to co-operate with law enforcement and regulatory authorities, and to stop other prohibited, illegal, or harmful activities;
- and any other purpose made known in this Privacy Policy or other policy.

We will not use or disclose this data for a secondary purpose unless you consent to us doing so, or under the circumstances involved we believe you would reasonably expect us to use or disclose the data for a secondary purpose and that that secondary purpose is related to the primary purpose. (SPACETALKUS, 2021b)

- **Does the Privacy Policy specify whether the information can be shared or sold to third parties?** There are mismatches between Spacetalk's main Privacy Policy and Spacetalk's Children's Privacy Policy.

Sale of Personal Information
Like most companies, we allow certain third-party advertising partners to place tracking technology such as cookies and pixels on our websites. This technology allows these advertising partners to receive information about your activities on our website, which is then associated with your browser or device. These companies may use this data to serve you more relevant ads as you browse the internet. Under some state laws, this type of sharing may be considered a "sale" of personal information. Spacetalk has no actual knowledge of any sales of personal information of minors under 16 years of age. (SPACETALKUS, 2021b)

When Information is Available to Others
We only share or disclose personal information collected from Children in a limited number of instances, including the following: We may share information with our service providers if necessary for them to support our "internal operations" (as defined by COPPA), including activities necessary for the site or service to maintain or analyze its functioning; perform network communications; authenticate users or personalize content; protect the security or integrity of the user, website, or online service; ensure legal or regulatory compliance; or fulfill a request of a child as permitted under COPPA; We may disclose personal information if permitted or required by law, for example, in response to a court

order or a subpoena. To the extent permitted by applicable law, we also may disclose personal information collected from Children (i) in response to a law enforcement or public agency's (including schools or children services) request; (ii) if we believe disclosure may prevent the instigation of a crime, facilitate an investigation related to public safety or protect the safety of a child using our sites or applications; (iii) to protect the security or integrity of our sites, applications, and other technology, as well as the technology of our service providers; or (iv) enable us to take precautions against liability; As otherwise permitted or required by COPPA or other applicable law. (SPACETALKUS, 2021a)

- **Does the Privacy Policy specify whether the data supply requested is voluntary or mandatory and the consequences of refusing to provide the requested information?** Yes. There is a list of practices in the main Spacetalk privacy policy, but not on the Children's privacy policy.

  With some of our products, such as Spacetalk™, we collect the geographical location of a smartphone or smartwatch. This data can be used to locate the carrier or wearer of the device. Location Data is collected solely for the purposes of assisting parents and caregivers to determine the location of the wearer or carrier of the device, under the explicit or implicit consent of that person. The services deal with location, so in order to work, the services need to know your location. Whenever you open and use/interact with our services on a mobile device, watch or go to one of our sites, we use the location information from your mobile or watch or other tracking device to tailor the services experience to your current location (we'll show your location). The services may also use your mobile device's background location to provide the services. If you have background location turned on, the services will, from time to time, inform us about your device's location even if you are not directly interacting with the services.

  Information You Instruct Us to Share

  We may also disclose your personal information to third parties to whom you expressly ask us to send the personal information to or to third parties you consent to us sharing your persona data with. If you choose to do so, your personal information and other information may be disclosed to such third parties and all information you disclose will be subject to the third-party privacy policies and practices of such third parties.

  Withdrawal of Consent, Access and Correction

  You may withdraw your consent for the collection, use or disclosure of your personal information by notifying our customer service team at privacy@spacetalkwatch.com, however, such withdrawal shall not have retroactive effect. You may also make a request to access

or correct your personal information by making a request in writing. (SPACETALKUS, 2021b)

- **Does the privacy policy specify the measures adopted by the application to ensure the confidentiality, integrity, and quality of Dice?** No.
- **Does the privacy policy specify how data is stored?** No.
- **Does the privacy policy mentioned agree with current law?** Yes. The main Spacetalk Privacy Policy has a considerably broad section regarding both the California Privacy Rights (under CCPA or otherwise) and Canadian Privacy Laws. The Children's Privacy Policy simply states that only the information "as otherwise permitted or required by COPPA or other applicable law" is disclosed.
- **Does the policy mention access for minors' deity?** The app is targeted at parents and guardians over 18 years of age.
- **Does the policy address privacy issues related to children?** The Spacetalk Children's Privacy Policy that very loosely covers children's privacy rights, though the main Privacy Policy provides some additional information that could be useful.
- **Does the policy clearly explain what happens to the user's data if he deletes the account?** No. The main privacy policy only states that the user has the right to request deletion of information under the California Privacy Rights (SPACETALKUS, 2021b). However, the company also informs that it may not comply with the request made by the user in certain circumstances.

In the **Rights of the Data Subject** category, Spacetalk provides enough information to the user in regards of their rights under state and international laws, coupled with more than one way to contact the company to handle privacy related matters.

- **Is the user free to access data about yourself even stored by application?** Could not determine.
- **Does the privacy policy specify the user rights?** Yes. The main privacy policy describes the user's rights under the California Consumer Privacy Act (CCPA) as well as Canadian privacy laws (SPACETALKUS, 2021b).
- **Does the privacy policy report data to contact the company?** There are two separate contacts provided by Spacetalk:

To exercise any of these rights, please contact us by emailing privacy@spacetalk.com or calling 1-833-SPACETALK (SPACETALKUS, 2021a)

Enquiries regarding this Privacy Policy or the personal information we may hold on you, should be made to our customer service team at privacy@spacetalkwatch.com. (SPACETALKUS, 2021b)

Regarding the **Changes to the Privacy Policy** category, Spacetalk explicitly states that it expects the user to check their privacy policy for any presented changes, failing to mention any other measures taken to assure that the changes reach the user.

- **How are changes in policies handled?** Spacetalk only discloses the following regarding changes to the privacy policy: *"We may update this Privacy Policy at any time. If we change, modify, amend, or replace this privacy policy, the last updated date will change."* (SPACETALKUS, 2021b)
- **What effect a change of privacy policy to an application imposes on the user?** No further information is provided.
- **How is the frequency of modification of the policy privacy?** The last modification dates to 15 October 2021 on the official website but no version history is provided.

The aspects of the **User Consent and Permission** category were covered based on the information provided by the privacy policy alone as we did not assess the application for the device.

- **What is the method of choosing the user for consent or not with the policy of privacy** Could not determine.
- **Does the user have the option of not agreeing with the applicable privacy policy?** Yes. The main Spacetalk privacy policy expands on the user's right to opt-out.
- **Is the user allowed to select what information it allows to be collected?** Could not determine.

A.3.4 TickTalk 4

For the **User Experience** category, it was noted that TickTalk provides very clear and straightforward ways for users to access the privacy policy on their website. On the TickTalk 4 page, a section named 'Privacy Policy' can be found among other product-related information; the device description also includes a link to the company's data handling practices and, lastly, a direct link to the policy can be found on the navigation bar. Furthermore, the privacy policy page is responsive and provide an even experience for those with low vision and other disabilities, albeit with minimal concerns.

- **Does the application present the Privacy Policy when the user accesses the platform?** Yes. There is a Privacy Policy section available on the main product page and a 'Policy' tab on the navigation bar.
- **How easy is it for the user to find the Privacy Policy in the App?** Easy. There is a readily available link at the top navigation bar of Ticktalk's website and a section on the main product page.
- **Is the document adequately translated to all the languages that the application supports?** The document is only available in English.
- **Is the Privacy Policy accessible to people with disabilities (PWD)?** The website presented a small issue related to colour contrast (green and white) which does not concern the policy text itself. No additional accessibility tools are provided on the privacy policy page.
- **Does the document present a readability level compatible with what the application users can read?** The readability score for the TickTalk privacy policy suggests that that individuals aged 16-17 should easily understand the text, meaning parents/guardians should be able to comprehend it.
- **Is the document responsive?** Yes, the document is responsive.

In regards to the **Privacy Policy Content** category, TickTalk takes a step further from Spacetalk (see A.3.3) and provides a rich amount of information to the user regarding their practices, from the elements involved in how data is processed to data security measures. Similar to the Gizmo privacy policy (see A.3.2), TickTalk also highlights their certification merits albeit with a greater level of detail, which could provide reassurance to the user. However, there could be some incongruities regarding selling personal data to third parties.

- **Is the Privacy Policy based on the assumption that the visit to the application implies the user's consent to the Policy, independent of the user reading the document or not?** Can't determine.
- **Does the policy specify clearly what data is collected?** Yes. Users are able to find a section with a comprehensive list of information that is collected and detailed concerns regarding children's personal information.

  WHAT INFORMATION DOES TICKTALK COLLECT FROM CHILDREN, AND HOW IS IT USED?

  Location-based Information Collected Through the TickTalk Service

The TickTalk Device and/or Services automatically and continuously collect information about the physical location of the TickTalk Device when activated. This information is acquired through numerous methods, including GPS and cell towers, which are enhanced over time as we follow the TickTalk Device, collect more information, and improve our tracking. You may not disable location-based data collection from the TickTalk Device and/or Services. We can access latitude and longitude in our backend of the TickTalk Device if needed by a Parent and/or Guardian with parental consent.

Child Personal Information Collected from Parent Created Account
Once a Parent and/or Guardian creates an Admin Account on the TickTalk App, they are prompted to create a Child Account to activate and begin using their TickTalk Device. The Parent (”Admin User”) can use the TickTalk App to locate and communicate with your Child, approve App Users (“Contacts”), manage communication preferences, and set privacy settings for your Child. Once a Parent creates an App account, they will be prompted to submit Child information to create a Child Account with the following information:
- Child’s Name and/or Nickname (optional): Your Child’s name is used for messaging, video calling, phone calls, and/or Greeting Cards sent to/from Parent-Approved App Users (”Contacts”). Parents and/or Guardians can opt to put in First Name, Nickname, or a non-identifying text as a placeholder.
- Child’s Birth Date (optional): Your Child’s Birth Date is used for Greeting Cards to send the Parent (”Admin User”) a reminder to send a Birthday Greeting Card. This information may be used for Research & Development purposes in a non-identifiable manner (i.e. information about our users that we combine so it no longer identifies or references an individual user). Parents and/or Guardians can also select None to not provide this information.
- Child’s Gender (optional): Your Child’s Gender is used for Research & Development purposes in a non-identifiable manner (i.e. information about our users that we combine so it no longer identifies an individual Child user). Parents and/or Guardians can also select None to not provide this information.
- Child’s Profile Picture (optional): Your Child’s Profile Picture is used for messaging, video calling, and phone calls sent to/from the Parent-Approved App Users (”Contacts”). Parents and/or Guardians can opt to put in a generic default avatar image as a placeholder.

We do not disclose any Personal Information about Children to third parties, except to subprocessors necessary to provide the Service, as required by law, or to protect the security of the Service or other users. We encourage you to read through our full list of Third Party Subprocessors for more information. (TICKTALK, 2022)

- **Does the Privacy Policy specify clearly how the data is collected?** Yes. TickTalk ex-

pands on the information that is automatically collected by combining different sources from both Children and Parents/Guardians in a dedicated section.

Information Collected Automatically from Children
TickTalk Devices will automatically collect Non-Personal Collective Information including:

- TickTalk Device Specific Identifiers such as Device IMEI number
- TickTalk Device Time and Usage Habits

TickTalk Devices will automatically collect Child Personal Information including:
TickTalk Device Precise Location (we do collect precise geolocation data from Children and the TickTalk Device will continuously collect information about the physical location when activated. We will not store or track your device location on an ongoing basis without your permission. We do not share precise geolocation data with third parties or advertisers. You may not disable location-based data collection from the TickTalk Device and/or Services and we will only access this information if given parental permission for troubleshooting purposes).

Information Collected Automatically from Customers And/Or Usrs Age 18+
Like most web-based services, we (or our subprocessors) may automatically collect information from your browser or your device when you use the TickTalk Website or TickTalk App. This information is necessary to improve performance and troubleshoot our Service and the TickTalk Website. It is possible at times when collecting Non-Personal Information through automatic means that we may unintentionally collect or receive Personal Information that is mixed in with Non-Personal Information. While we make efforts to prevent this type of incidental data collection, the possibility does exist. If we happen to combine any automatically-collected information with Personal Information, we will treat the combined information as Personal Information, which will be protected by this Privacy Policy.

Information Received from Third Party Sources
If we receive adult Personal Information from third parties, we will handle it in accordance with this Privacy Policy. If we directly combine information we receive from other third parties with Personal Information that we collect through the Service or TickTalk Website, we will treat the combined information as Personal Information and handle it in accordance with this Privacy Policy. (TICKTALK, 2022)

- **Does the Privacy Policy clearly specify if the application does use some tool or external service?** Yes. The privacy policy details how third parties involved in operating the services for the device have access to the information and the respective purposes. Addi-

tionally, a link is provided to access their list of third-party subprocessors[33].

Third-Party Services

TICKTALK DEVICES AND/OR TICKTALK PARENTAL CONTROL APP
We do not share any Child Personal Information with third-party services. All TickTalk Services including TickTalk Devices and the TickTalk Parental Control App are managed and maintained internally by TickTalk Tech LLC without the aid or assistance of third parties. If a third party technology is used on our Services, such as iHeartRadio Family, we integrate the third party API into our backend to ensure our data collection, usage, and protection are in line with this Privacy Policy.

We do use Amazon's AWS Cloud Computing Services to remotely store Child Personal Information that has gone through end-to-end encryption. All Personal Information and Data will go through encryption before being sent and we will never share Personal Information without encryption.
It is important to us that you have full transparency over the third-party services we work with and the specific information they have access to. We encourage you to read through our full list of Third Party Subprocessors for more information.

GIGS WIRELESS, LLC (CELLULAR SERVICE PROVIDER)
TickTalk Tech LLC provides a free TickTalk Wireless SIM card with every purchase for U.S. customers provided by Gigs Wireless, LLC. Gigs Wireless, LLC provides cellular service for TickTalk Devices, similar to your personal cellular provider on your personal cell phone.
Upon receiving a TickTalk order, the Parent and/or Guardian will be prompted to activate the included SIM card here where they will create a parent account, select a monthly plan, and enter payment information. Gigs Wireless, LLC will then provide a cellular phone number for your Child's TickTalk Device. Gigs Wireless, LLC has access to the information necessary to provide cellular service on your Child's TickTalk Device.

Gigs Wireless, LLC will be able to access: Your Child's Gigs Wireless, LLC SIM Card ICCID Identifying Number; Your Child's Device Phone Number; Your Child's Device IMEI Identifying Number; Your Child's Device Data Usage; Your Child's Device Voice Call Logs at Network Level including Call Duration, Other Party Phone Number, and Time Stamps for Billing Purposes; Your Child's Device SMS Text Logs at Network Level including Other Party Phone Number and Time Stamps for Billing Purposes

[33] THIRD PARTY SERVICE PROVIDERS – My TickTalk <https://www.myticktalk.com/pages/third-party-service-providers>

For Parents and/or Guardians who have created and set up a TickTalk Wireless phone number for your Child's TickTalk Device, Gigs Wireless, LLC will be able to view: Billing Name & Address as provided by the Parent and/or Guardian; Email Address as provided by the Parent and/or Guardian; Payment Information as provided by the Parent and/or Guardian.

RED POCKET (CELLULAR SERVICE PROVIDER)
TickTalk Tech LLC provides a free SIM card with every purchase for U.S. customers provided by Red Pocket. Red Pocket provides cellular service for TickTalk Devices, similar to your personal cellular provider on your personal cell phone.

Red Pocket will be able to access: Your Child's Red Pocket SIM Card ICCID Identifying Number; Your Child's Device Phone Number; Your Child's Device IMEI Identifying Number; Your Child's Device Data Usage; Your Child's Device Voice Call Logs at Network Level including Call Duration, Other Party Phone Number, and Time Stamps for Billing Purposes; Your Child's Device SMS Text Logs at Network Level including Other Party Phone Number and Time Stamps for Billing Purposes.

For Parents and/or Guardians who have created and set up a Red Pocket phone number for your Child's TickTalk Device, Red Pocket will be able to view: Billing Name & Address as provided by the Parent and/or Guardian; Email Address as provided by the Parent and/or Guardian; Payment Information as provided by the Parent and/or Guardian. (TICKTALK, 2022)

- **Does the Privacy Policy specify how the company can use the collected data?** Yes. Similar to the previous questions, TickTalk also provides a separate section to outline how they can utilise and handle personal data, especially children's data.

  How We Use the Information We Collect

  We do not sell or rent any of your or your Child's Personal Information to any third party for any purpose, including for advertising or marketing. Third-party advertising is not permitted on our Service and Personal Information collected from Children is never used for behaviorally-targeted advertising to Children. We will only use your information, including Personal Information, collected through our Service for the purposes described in this Privacy Policy, unless you have specifically consented to another type of use, either at the time the information was collected or through another form of consent or notification. We may use the information, including Personal Information, from adult users we collect to:

Provide and/or personalize the TickTalk Services, Website, Devices, or content and experiences for you
- Communicate with you about your use of the Service, your account, or transactions with us
- Respond to your emails, questions, requests, complaints and provide customer service
- Send you information about new features or changes to our Service or policies
- Optimize or improve the TickTalk Website, Devices, Services, and operations and develop new products
- Develop and enhance our products and services with the use of aggregated data or de-identified data to use for research and development purposes provided that any disclosures of such data do not specifically identify you, your Child, your Child's TickTalk Device, and/or your precise location
- Send you security alerts and support messages and otherwise facilitate your use of the Service and TickTalk Website
- Combine with data from other sources outside of your use of the TickTalk Service, such as data obtained from Wi-Fi access points within range of your Child's TickTalk Device
- For safety and security reasons, such as detecting, investigating, and preventing activities that may violate our policies or be illegal
- Provide Parents with information about announcements, offers, promotions, and new products
- For any other purpose for which the information was collected such as fulfilling product orders

We process this information to improve the TickTalk Website, the Service, and our users' experience with it, protect the Service and the TickTalk Website, and comply with applicable laws. We will process your Personal Information with the legitimate interest of offering your new products or services that may be of interest to you. You may opt out of receiving marketing communications from us by unsubscribing to email marketing or by changing your notification settings in your TickTalk App account. (TICKTALK, 2022)

- **Does the Privacy Policy specify whether the information can be shared or sold to third parties?** There are contradictions in TickTalk's Privacy Policy, as it could be implied that Ticktalk could be combining users' data with information collected from third parties for practices that could categorise as 'sale' per the definition proposed by the California Consumer Protection Act (CCPA). Although the company says for users 18+ that they *"will never sell or rent your Personal Information to advertisers or other third parties"* (TICKTALK, 2022), TickTalk also says that they *"share certain personal information with third party ad networks for purposes of behavioral advertising, including: Commercial and Financial Information, Internet Activity, Online Identifiers, and Personal*

Identifiers. This allows us to show you ads that are more relevant to you." (TICKTALK, 2022)

We do not share any Child Personal Information publicly. Children Users cannot share any information publicly outside of the TickTalk Device or Services. The statements that we make regarding the information we collect from or about Children and how we use this information apply equally to all Children regardless of their age. Accordingly, where this Privacy Policy references Children or any information collected from or about Children our Privacy Policy applies to Children under 13 years of age as well as Children 13 years of age and above;
We do not share your Child's Personal Information with our subprocessors unless it has previously gone through end-to-end encryption, is unreadable by the subprocessor, and is necessary to provide our services;
All Child Personal Information, except for Device information and location services, is provided by the Parent ("Admin User") upon creation of a TickTalk App account. There are two types of storage for Personal Information:
- Locally on your Child's TickTalk Device which we cannot view and/or access
- Non-Locally on the parental control TickTalk App which we store externally within the AWS Cloud Server and can view and/or access particular Personal Information

Parent-Approved App Users ("Contacts") who have Full Access have the same access level as the Parent ("Admin User"). Full Access App Users are typically Parents, Guardians, and close family members (i.e. Grandparents) who need access to locating capabilities or the ability to edit your Child's TickTalk Device settings.
TickTalk Tech LLC does not store or share any Child Personal Information in the Facebook service. (TICKTALK, 2022)

- **Does the Privacy Policy specify whether the data supply requested is voluntary or mandatory and the consequences of refusing to provide the requested information?**
  Yes. The Privacy Policy has two separate sections: one for information provided by the users and another for information automatically collected by the devices. They very loosely cover what happens if you do not provide consent.

  OBJECT, RESTRICT, OR WITHDRAW CONSENT
  Where you have provided your consent to TickTalk Tech LLC for the processing of your Personal Information by us you may withdraw your consent at any time by changing your account settings or by sending a communication to us at privacy@myticktalk.com specifying which consent you are withdrawing or by making a request in our Privacy Center. (TICKTALK, 2022)

- **Does the privacy policy specify the measures adopted by the application to ensure the confidentiality, integrity, and quality of Dice?** Yes. There is a quite extensive section with measures taken by TickTalk to assure data security.

  DATA SECURITY
  The security of your Personal Information is important to us. To prevent unauthorized access, disclosure, or improper use of your information, and to maintain data accuracy, we've established physical, technical, and administrative safeguards to protect the Personal Information we collect. In particular:

  - We periodically review our information collection, storage, and processing practices, including physical security measures, to guard against unauthorized access to systems.
  - We perform application security testing, penetration testing, conduct risk assessments, and monitor compliance with security policies. These vulnerability tests are performed for every TickTalk App and TickTalk Device operating system (OS) update, typically occurring every other month to quarterly.
  - When you enter any information anywhere on the Service, we encrypt the transmission of that information using secure socket layer technology (SSL) by default.
  TickTalk Tech LLC's database where we store your Personal Information is encrypted at rest, which converts all Personal Information stored in the database to an unintelligible form.

  We ensure passwords are stored and transferred securely using encryption and salted hashing. TickTalk's Website and the Service are hosted by third-party subprocessors at separate facilities, with whom we have a contract providing for enhanced security measures. We restrict access to Personal Information to authorized TickTalk Tech LLC employees who need to know that information to process it for us, and who are subject to strict confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

  Although we make concerted good faith efforts to maintain the security of Personal Information, and we work hard to ensure the integrity and security of our systems, no practices are 100% immune, and we can't guarantee the security of information due to the inherent open nature of the Internet and wireless communications. We cannot guarantee that your personal information will be completely free from unauthorized access by third parties, such as when transferred over or through systems not within our exclusive control. Your use of the TickTalk Services demonstrates your assumption of this risk. Outages, attacks, human error, system failure, unauthorized use, or other factors may compromise the security of user information at any time.

If we become aware of a systems security breach by an unauthorized party or that any user data was used for an unauthorized purpose, we will comply with relevant state and other data breach laws. We will notify users of any breach resulting in an unauthorized release of data electronically, at minimum, and without unreasonable delay so that you may take appropriate steps. The notification will include the date of the breach, types of information that were subject to the breach, a general description of what occurred, and steps TickTalk Tech LLC is taking to address the breach. We may also post a notice on the TickTalk Website or elsewhere on the Service, and may send an email to you at the email address you have provided to us. (TICKTALK, 2022)

- **Does the privacy policy specify how data is stored?** Yes. There are multiple instances where the policy addresses data storage and from where they can be accessed.

  What Children's Information is Visible to TickTalk Tech LLC?

  All Child Personal Information, except for Device information and location services, is provided by the Parent ("Admin User") upon creation of a TickTalk App account. There are two types of storage for Personal Information:
  - Locally on your Child's TickTalk Device which we cannot view and/or access;
  - Non-Locally on the parental control TickTalk App which we store externally within the AWS Cloud Server and can view and/or access particular Personal Information.

  Child Personal Information Stored Within Our Devices
  We follow the Federal Trade Commission's (FTC) Children's Online Privacy Protection Act ("COPPA") rules for parental consent prior to a Parent and/or Guardian activating and setting up our Devices. Before creating an account for a Child and using our TickTalk Devices, Parents and/or Guardians must certify that they reviewed and consented to our Privacy Policy and that we collected the appropriate parental consent. We rely on verifiable parental consent from the Parent and/or Guardian to use TickTalk's Services and require consent via email and within our TickTalk App upon the Parent account registration process.

  Once the Parent ("Admin User") has created a Child Account and provided us with verifiable parental consent, then the following information may be collected from your Child locally on their TickTalk Device. This data is stored locally on the Device and is not available in the TickTalk App or to TickTalk Tech LLC. Your Child can also choose to share this information with Parent-Approved App Users ("Contacts") and/or other TickTalk Devices your Child has added as a Contacts using the Add Friends feature:
  - Child Created Photographs and Videos: Photos (which may contain Personal Informa-

tion) and/or Videos can be stored locally on the Device. Due to size, videos cannot be shared with any Contacts and will only be stored locally on your Child's TickTalk Device.
- Child Created Message Content and Voice Recordings: Your Child may create and send messages and voice recordings (which also may contain Personal Information) in our end-to-end encrypted Secure Messaging Center with Contacts.
- Child Submission of Photo or Other Image via the Secure Messaging Center: Your Child can share photos, emojis, GIFs, voice recordings, preset text responses, or other representations of themselves within the Secure Messaging Center with Contacts. Your Child may share Photos in our end-to-end encrypted Secure Messaging Center with Contacts. (TICKTALK, 2022)

- **Does the privacy policy mentioned agree with current law?** Yes. TickTalk includes a dedicated section to expanding on their compliance with the CCPA.

  The California Consumer Privacy Act (CCPA) provides California residents with specific rights regarding their personal information. To read our California Privacy Notice (CCPA) in its entirety, please visit our Privacy Center.

  Our Privacy Center describes your rights as a California resident including but not limited to:
  - Information We Collect
  - Information You Provide To Us
  - Information Collected Automatically
  - Information From Other Sources
  - How Long We Keep Your Data
  - How We Share And Disclose Information including Information Disclosed for Business or Commercial Purposes in the Last 12 Months and Categories of Parties Disclosed To
  - Collection and Disclosure of Personal Information Business and
  - Commercial Purposes for Collection Information "Sharing" and "Selling"
  - CCPA Rights including Your Right to Know, Right to Delete, Right to Non-Discrimination, and Right to Opt-Out
  - Request Verification
  - Authorized Agent
  - Contact
  - Notice of Financial Incentive. (TICKTALK, 2022)

- **Does the policy mention access for minors' deity?** The app is targeted at parents and guardians over 18 years of age.

- **Does the policy address privacy issues related to children?** Yes.

TICKTALK CERTIFICATIONS, COMMITMENTS & ADHERENCE
TickTalk Tech LLC has also committed to a set of principles intended to safeguard Children's privacy, including responsible protection and transparent handling of Children's Personal Information.

We participate in the iKeepSafe Safe Harbor program. TickTalk Tech LLC has been granted the iKeepSafe COPPA Safe Harbor seal signifying its Website, Devices, and Apps have been reviewed and approved for having policies and practices surrounding the collection, use, maintenance, and disclosure of Personal Information from Children consistent with the iKeepSafe COPPA Safe Harbor program guidelines.
TickTalk participates in the iKeepSafe Safe Harbor program. If you have any questions or need to file a complaint related to our privacy policy and practices, please do not hesitate to contact the iKeepSafe Safe Harbor program at COPPAprivacy@ikeepsafe.org

UNITED STATES OF AMERICA
The Service and TickTalk Website is hosted, maintained, and operated in the United States. By using the Service or the TickTalk Website, you freely and specifically give us your consent to export your Personal Information to the United States and to store and/or use in the United States as specified in this Privacy Policy. We follow the Federal Trade Commission's (FTC) Children's Online Privacy Protection Act ("COPPA") rules for parental consent prior to a Parent and/or Guardian activating and setting up our Devices. You understand that data stored in the United States may be subject to lawful requests by the courts or law enforcement authorities in the United States.
For international users using the TickTalk Services, you further acknowledge that the United States may not have the same data protection laws as the country from which you provided your Personal Information and that TickTalk Tech LLC may be compelled to disclose your Personal Information to U.S. authorities. (TICKTALK, 2022)

- **Does the policy clearly explain what happens to the user's data if he deletes the account?** Yes. The 'Object, Restrict, or Withdraw Consent' offers details on the measures taken by the company regarding the deletion of data and the amount of time they will retain that data for once the request is consented.

If for some reason you ever want to delete your account or your Child's Account, if you are the Parent and/or Guardian, you can do so at any time:
- To Deactivate/Delete Your Parent ("Admin User") App Account: You may at any time deactivate or delete your Parent ("Admin User") App Account by visiting the TickTalk App under Settings > My App > Account Deactivation.
- To Deactivate/Delete An Approved App User (Contact): You may at any time deactivate or delete an Approved App User (Contact) by visiting the TickTalk App under Settings

> My TickTalk > Approved App Users > Unbound. You may also change the individual access level (Full Access or Limited Access) of an Approved App User at any point by visiting the TickTalk App under Settings > My TickTalk > Approved App Users.
- To Deactivate/Delete Child Account: You may at any time deactivate or delete your Child's TickTalk Device account by visiting the TickTalk App under Settings > My TickTalk > Enable Watch Features > Deactivate Watch and toggling on.
- To Perform A System Reset On Your TickTalk Device: You can perform a system reset on your Child's TickTalk Device by visiting the TickTalk App under Settings > My TickTalk > System Reset. You can also reset your Child's TickTalk Device locally by going into the watch Settings > Reset. This will clear all personal data from your Child's TickTalk Device to reset to factory settings.

When you delete your Parent or Child account, we delete all profile information and any other content you provide in your profile (such as your name and/or nickname, password, email address, phone number, and profile photos), data (such as message content, phone book contacts, and App Users Contacts) and information collected through mobile permissions you've granted.

To delete your Child's TickTalk Device account, the Parent and/or Guardian can perform a System Reset from the TickTalk App and unbound your Child's TickTalk Device from the TickTalk App to reset to factory settings without any Child Personal Information. Any Personal Information that you have shared with Parent-Approved Contacts or content your Contacts may have copied and stored is not a part of your account and may not be deleted when you delete your account.

We aim to protect your information to safeguard you from malicious or accidental destruction. Because of this, even after you update or delete Personal Information you have provided us from our Service or the TickTalk Website, your Personal Information may be retained in our backup files or archives for a reasonable period of time for legal purposes or for so long as is necessary in light of the purposes for which such records were collected or legitimately further processed.

DESTROYING & DELETING PERSONAL INFORMATION
We can delete and destroy data with consent from the Parent and/or Guardian if they are the Admin User, or the first person to pair with the TickTalk Device. In this case, we would take the following steps to confirm the person requesting to review or delete your Child's data is the Parent and/or Guardian including:
- Verifying the purchase within our TickTalk Website or Amazon Marketplace
- Verifying the individual contacting us is the Admin User or the first person to pair with

the TickTalk Device
- Verifying the TickTalk Device IMEI and/or TTID identifying number

If the individual contacting TickTalk Tech LLC verifies their identity as the Parent and/or Guardian of the Child User of the TickTalk Device, we can:
- Perform a system reset from the TickTalk backend to delete all Personal Information and data on both the TickTalk Device and TickTalk App
- Unbound all Parent-Approved App Users ("Contacts")
- Deactivate the Device to prevent any further communication with the TickTalk Device

Once we have performed these steps, all Child Personal Information, Parent and/or Guardian Personal Information, and Parent-Approved Contacts Personal Information will be immediately deleted and destroyed from our backend as well as on the TickTalk App and Device. (TICKTALK, 2022)

Regarding the **Rights of the Data Subject** category, TickTalk provides enough information to the user in regards of their rights under regulations in the United States, coupled with more than one way to contact the company to handle privacy related matters.

- **Is the user free to access data about yourself even stored by application?** Yes. The TickTalk privacy policy provides ways for the parent/guardian to request access to the information retained by the device and/or application.

  For any information that the Parent and/or Guardian asks TickTalk Tech LLC to access, review, correct, and/or delete on your behalf, we will use commercially reasonable efforts to process requests in a timely manner consistent with applicable law. We will ask you to verify your identity as the Parent and/or Guardian, for example by requiring that you provide acceptable forms of personal identification, providing us your device identifying numbers, or your purchase order number for us to cross-reference with our records. (TICKTALK, 2022)

- **Does the privacy policy specify the user rights?** Yes. The privacy policy addresses users' rights under the CCPA coupled with a general list of rights pertinent to the user.

  Transparency and Your Rights
  We try to be as transparent as possible about the information we collect so that you can make an educated decision on how your information is used. You can access, correct, or delete this information at any time. You may also object, restrict, or withdraw consent where applicable for the use of Personal Information you have provided to us. We also make the Personal Information you share through our Service or the TickTalk Website

available and provide easy ways for you to contact us.
You may exercise any of the rights described in this section by contacting us at privacy@myticktalk.com or making a request here. We will ask you to verify your identity before taking any action on your request. (TICKTALK, 2022)

- **Does the privacy policy report data to contact the company?** There are two separate ways of contacting TickTalk and a contact page[34] provided in the privacy policy.

  Contacting TickTalk
  If you have questions or concerns about this Privacy Policy or our collection, use, or disclosure of your Personal Information, please contact us in one of the following ways:
  Email: privacy@myticktalk.com
  Phone: 1-(844)-260-4051
  Mailing Address:

  TickTalk Tech LLC
  ATTN: Privacy Policy
  565 West Lambert Road, Unit B
  Brea, CA 92821 (TICKTALK, 2022)

Regarding the **Changes to the Privacy Policy** category, TickTalk also explicitly states that it expects the user to check their privacy policy periodically and, in the case of any changes, parents and guardians should be notified to obtain consent over the presented modifications.

- **How are changes in policies handled?** Ticktalk claims that users should check their privacy policy periodically for changes.

  We encourage you to review this Privacy Policy from time to time, to stay informed about our collection, use, and disclosure of Personal Information through the Service and TickTalk Website. If you don't agree with any changes to the Privacy Policy, you may delete and/or deactivate your account at any time. By continuing to use the Service or the TickTalk Website after the revised Privacy Policy has become effective, you acknowledge that you accept and agree to the current version of the Privacy Policy. (TICKTALK, 2022)

- **What effect a change of privacy policy to an application imposes on the user?** They state on their main Privacy Policy that *"in addition, if we ever make significant changes to the types of Personal Information we collect from Children, or how we use it, we will notify Parents and/or Guardians to obtain parental consent and notice for any material changes to policy or new data collection practices.* (TICKTALK, 2022)

[34] CONTACT US - My TickTalk <https://www.myticktalk.com/pages/contact>

- **How is the frequency of modification of the policy privacy?** The last modification to the Privacy Policy is dated 30 December 2022, but there is no version history available on the website.

The aspects of the **User Consent and Permission** category were covered based on the information provided by the privacy policy alone as we did not assess the application for the device.

- **What is the method of choosing the user for consent or not with the policy of privacy?** Could not determine.
- **Does the user have the option of not agreeing with the applicable privacy policy?** Yes. The privacy policy expands on the user's right to opt-out.
- **Is the user allowed to select what information it allows to be collected?** The TickTalk privacy policy describes what kind of optional information parents and guardians can willing refuse, but there are no details regarding all the opting-out options.

- Child's Name and/or Nickname (optional): Your Child's name is used for messaging, video calling, phone calls, and/or Greeting Cards sent to/from Parent-Approved App Users (''Contacts''). Parents and/or Guardians can opt to put in First Name, Nickname, or a non-identifying text as a placeholder.
Child's Birth Date (optional): Your Child's Birth Date is used for Greeting Cards to send the Parent (''Admin User'') a reminder to send a Birthday Greeting Card. This information may be used for Research & Development purposes in a non-identifiable manner (i.e. information about our users that we combine so it no longer identifies or references an individual user). Parents and/or Guardians can also select None to not provide this information.
- Child's Gender (optional): Your Child's Gender is used for Research & Development purposes in a non-identifiable manner (i.e. information about our users that we combine so it no longer identifies an individual Child user). Parents and/or Guardians can also select None to not provide this information.
- Child's Profile Picture (optional): Your Child's Profile Picture is used for messaging, video calling, and phone calls sent to/from the Parent-Approved App Users (''Contacts''). Parents and/or Guardians can opt to put in a generic default avatar image as a placeholder. (TICKTALK, 2022)

A.3.5 Huawei Watch Kids 4 Pro

For the **User Experience** category, it was observed that, similar to Verizon (see A.3.2) and Spacetalk (see A.3.3), Huawei does not provide straightforward ways for the user to easily

access their privacy policies. On the main business privacy statement, users can find a single section briefly covering concerns with minors' personal data processing along with a link to a children's business privacy statement. Nevertheless, the privacy policy page is responsive and provide an even experience for those with low vision and other disabilities, albeit with minimal concerns.

- **Does the application present the Privacy Policy when the user accesses the platform?** There are no links to the Privacy Policy anywhere on the main product page.
- **How easy is it for the user to find the Privacy Policy in the App?** Hard. The main product page has no links to its specific Privacy Policy and the Children's Privacy Policy can only be found under one of the categories on the main Privacy Policy, which already is not easy to be located.
- **Is the document adequately translated to all the languages that the application supports?** The Privacy Policy is available in multiple languages, but the Children's Privacy Policy is only available in English.
- **Is the Privacy Policy accessible to people with disabilities (PWD)?** The website presented a small issue related to colour contrast (grey and white) which does not concern the policy text itself. No additional accessibility tools are provided on the privacy policy page.
- **Does the document present a readability level compatible with what the application users can read?** No. The readability score for the main Huawei privacy policy suggests that that individuals aged 16-17 should easily understand the text, meaning parents/guardians should be able to comprehend it. However, the Children's privacy policy's readability score suggests the text should be understood by individuals aged 22-23, indicating a much more complex list of policies. It is particularly concerning considering Huawei indicates in that same Children's policy privacy that children should read the text and request their parents/guardians to follow suit.

  Children must ask their guardians to carefully read this Statement and seek permission or guidance from their guardians before using our products or services or providing information to us. (HUAWEI, 2022a)
- **Is the document responsive?** Yes, the document is responsive.

The category of **Privacy Policy Content** brings to light that Verizon provides very minimal information to the user regarding its data practices. There is no expanding into specific details, especially in regards to children, despite having a privacy policy aimed at outlining children-related policies. Furthermore, it affirms that *"Gizmo's privacy practices are covered*

by Verizon's Privacy Policy as well as the practices described here" (VERIZON, 2023a), potentially aggravating users' confusion and causing a spectrum of mismatching information. Despite claiming that *"in the event of a conflict between the two policies, the practices described in this policy govern when you are using Gizmo products and services"* (VERIZON, 2023a), it further suggests that there could be underlying uninformed practices.

- **Is the Privacy Policy based on the assumption that the visit to the application implies the user's consent to the Policy, independent of the user reading the document or not?** Could not determine.
- **Does the policy specify clearly what data is collected?** Huawei provides a list of information they collect although not clearly.

  Personal information refers to any type of information recorded electronically or otherwise relating to an identified or identifiable natural person, excluding information that has been anonymised. We may collect your personal data when you use our products or services or interact with us. Different types of data will be collected, depending on the service you use and your interactions with us. In some cases, you can choose not to provide such data, but this may prevent us from providing you with corresponding products or services, or may mean that we cannot respond to or resolve any issues you have raised. (HUAWEI, 2022b)
- **Does the Privacy Policy specify clearly how the data is collected?** Once again, the company provides different information in each privacy policy. In the Children's privacy policy, Huawei informs that both that and the main privacy policy are complementary, which could also cause further confusion.

  I. How Huawei Collects and Uses Children's Personal Information
  When you and any child under your guardianship use our products or services, the child's personal information may be required. You and the child under your guardianship are not obliged to provide the child's personal information to Huawei. However, in some cases, if you and the child choose not to provide it, Huawei will not be able to provide you or the child with the products or services concerned or respond to or resolve issues encountered by you or the child. Huawei will only collect and use children's personal information for the purposes described in this Statement. The following illustrates the children's personal information that we may collect and use:

  (1) Creating a child account. When you create a HUAWEI ID for any child under your guardianship or the child creates a HUAWEI ID by themselves, we need you or the child to enter the child's date of birth, HUAWEI ID (mobile number/email address), nickname,

and password. To comply with requirements of laws and regulations, Huawei may take measures to verify that the user who is creating the child account is a parent of the child (including the father, mother, or other guardian). For this purpose, we may ask you to provide the login password of your current parent account for confirmation so we can verify your parent identity. After you create a HUAWEI ID for your child, we will link your account with the child account, and your child will be able to use their HUAWEI ID to access our products or services.
(2) Enabling Child/Youth mode. When you select Child/Youth mode, we may further collect your account information or contact information and use the information for purposes such as verifying your identity. We may also collect your device information such as the management password and device identifiers (for example, IMEI and SN) to protect the personal information rights and interests of you and the child under your guardianship.
(3) Others. As you and the child under your guardianship are using our products or services, we may also collect and use other personal information of the child. For details about the purpose, method, and scope of the processing, see the Huawei Consumer Business Privacy Statement and privacy statements (if any) for the specific products or services concerned.
(4) We will inform you additionally if we need to collect personal information of you or the child under your guardianship beyond the above scope. (HUAWEI, 2022a)

We will collect and use your personal data only for the purposes described in this Statement and Product Privacy Notice. The following are some examples of personal data we may collect:

(1) Personal data that you provide to Huawei
You need to register a HUAWEI ID to enjoy certain functions or services. When you register a HUAWEI ID or log in to your HUAWEI ID to shop online, download software, or purchase services, we may ask you to provide relevant personal data, such as your name, email address, mobile number, order information, shipping address, and payment method.
Some Huawei products allow you to communicate and share information with others. When you use a Huawei product to share contents with your family and friends, you may need to create an open HUAWEI ID profile, which includes your nickname and avatar. We may also collect information about your family and friends, such as their names, email addresses, and phone numbers. We will take appropriate and necessary measures to ensure their communications security.
In order to meet the requirements of certain jurisdictions for real-name account registration, game addiction prevention systems, and Internet payment as well as other requirements, we may ask you to provide identity proofs issued by local governments, or relevant

card information that can authenticate your identity.
(2) Information that Huawei collects when you use services
When you use our products and services, we will collect your device information and how you and your device interact with our products and services. Such information includes:
a. Device and app information, such as the device name, device identifier, device activation time, hardware model, operating system version, app version, software identifier, and device and app settings (such as region, language, time zone, and font size).
b. Mobile network information, such as the public land mobile network (PLMN) provider ID, geographical location (cell ID of the area where the device is located), and Internet protocol (IP) address.
c. Log information. When you use Huawei services or view Huawei-provided content, we will automatically collect and log some information, such as the time of access, access count, IP address, and event information (such as errors, crashes, restarts, and updates).
d. Location information. When you access certain location-based services (such as perform searches, use navigation software, or view the weather for a specific location), we will collect, use, and process the approximate or precise location of your device. Such information may be obtained through the GPS, WLAN, or service provider network ID. We will ask you to select the apps for which you want to enable location services. You can refuse to share your location by disabling the corresponding permission in your device settings.
e. Information stored in the cloud. For example, the information you upload to the cloud will be stored on our servers for rapid access and sharing between devices. No one has access to such information without your permission.
(3) Information from third-party sources
When permitted by local laws, we may also obtain other information about you, your device, or service usage from public or legitimate commercial sources. For example, we obtain your information from the third party when you log in to our website through a third-party social media account, or when your contact information is uploaded by others who use our communication services. (HUAWEI, 2022b)

- **Does the Privacy Policy clearly specify if the application does use some tool or external service?** Yes, though the statements are oftentimes vague. Huawei also explicity informs the user that they take no responsibility for how third parties' data processing practices.

V. Third-Party Links, Products, and Services
Huawei's websites, apps, software, products, and services may contain links to third-party websites, products, and/or services. Huawei's products and services may also use or provide products or services from third parties, such as third-party apps available on HUAWEI AppGallery. All links to third-party websites, products, and services are pro-

vided for users' convenience only. Please note that the third party may process children's information. You are advised to carefully read and fully understand its applicable children's privacy protection statements before allowing the child under your guardianship to use its products or services. (HUAWEI, 2022a)

To ensure smooth user experience, Huawei websites, apps, products, and services may contain links to third-party websites, products, and services. Huawei's products and services may also use or provide products or services from third parties, such as third-party apps available on HUAWEI AppGallery. Huawei does not have control over third-party websites, products, and services, but you can choose whether to access these links.
Huawei also has no control over the privacy or data protection policies of third parties, as such third parties are not bound by this Statement. Before submitting personal data to third parties, please read and refer to their privacy or data protection policies. (HUAWEI, 2022b)

- **Does the Privacy Policy specify how the company can use the collected data?** The main privacy policy offers a vague list of ways Huawei can utilise users' personal data. Similar to Spacetalk (see A.3.3), they also present a confusing statement to bookend their policy claiming that data can be used for *"other purposes described in the Product Privacy Notice"* (HUAWEI, 2022b) without further clarification.

2. How Huawei Uses Your Personal Data

We use your personal data only on a legal basis. According to applicable local laws, we may use your personal data for the following purposes under one of the legal bases: your consent; necessary to perform/enter into a contract between you and Huawei; necessary to protect the legitimate interests of you or others; necessary to fulfil legal obligations; and necessary to protect the legitimate interests of enterprises:
(1) Register and activate our products or services that you have purchased;
(2) Register your HUAWEI ID so that you can enjoy a wider range of functions;
(3) Deliver, activate, or verify the products and services you have requested, or perform changes and provide technical support and after-sales services for such offerings at your request;
(4) Notify you of operating system or app updates and installations;
(5) Provide individualized user experience and content;
(6) After obtaining your consent or receiving your request, send you information about products and services you might be interested in, invite you to our promotional activities and market surveys, or send marketing information to you;
(7) Carry out internal audit, data analysis, and research; analyse business operation efficiency and measure market shares; and improve our products and services;

(8) Troubleshoot problems after you send error details to us;
(9) Synchronise and store the data you have uploaded or downloaded, as well as the data needed for upload and download operations;
(10) Improve our loss prevention and anti-fraud programs;
(11) Comply with applicable local laws/regulations, for example, fulfil e-commerce platform management obligations, or comply with legal government requirements;
(12) Other purposes described in the Product Privacy Notice. (HUAWEI, 2022b)

- **Does the Privacy Policy specify whether the information can be shared or sold to third parties?** There are mismatches between Huawei's Privacy Policy and Huawei's Children's Privacy Policy, and the purposes and/or recipients for sharing children's personal data are not clearly specified on either privacy policy .

  If Huawei shares or transfers children's personal information to a third party, Huawei will perform a security assessment of the sharing practice and the recipient, and sign pertinent agreements, such as a data protection agreement, with the third party.

  V. Third-Party Links, Products, and Services
  Huawei's websites, apps, software, products, and services may contain links to third-party websites, products, and/or services. Huawei's products and services may also use or provide products or services from third parties, such as third-party apps available on HUAWEI AppGallery. All links to third-party websites, products, and services are provided for users' convenience only. Please note that the third party may process children's information. You are advised to carefully read and fully understand its applicable children's privacy protection statements before allowing the child under your guardianship to use its products or services. (HUAWEI, 2022a)

  2. Sharing
  Sharing refers to the process in which we provide personal data to other personal data processors, and both parties can independently determine the data processing purposes and methods. We will not share your personal data with external parties, except in the following cases:
  (1) Sharing with your consent: After obtaining your consent, we will share your authorised personal data with third parties designated by you. (HUAWEI, 2022b)

- **Does the Privacy Policy specify whether the data supply requested is voluntary or mandatory and the consequences of refusing to provide the requested information?** Statements are very vague regarding consent of data provision. Even though Huawei claims to implement a Children's privacy by default (see 2.2.1) approach, the information provided to the user does not specify how the company ensures the implementation.

We protect children's privacy by default. Our products or services automatically disable personalized ads and direct marketing features and provide content that is appropriate for children when use by a child is detected. Your consent will be sought before your child's personal information is used for the purpose of providing a personalized experience for your child or improving our services. To help you protect the child under your guardianship, we also provide some parental control features, including Access restrictions, Time management, and Ask to buy. You can better protect the child under your guardianship by setting the duration or period for the child to use each app, their access to specific apps or services, or access to content based on their age group, as well as approving or denying their payment operations. (HUAWEI, 2022a)

(1) Sharing with your consent: After obtaining your consent, we will share your authorised personal data with third parties designated by you.
(6) After obtaining your consent or receiving your request, send you information about products and services you might be interested in, invite you to our promotional activities and market surveys, or send marketing information to you. (HUAWEI, 2022b)

- **Does the privacy policy specify the measures adopted by the application to ensure the confidentiality, integrity, and quality of Dice?** In regards to security measures, the only available information outlines that Huawei has *"in response to possible risks, such as personal data leakage, damage, and loss, we have developed several mechanisms and control measures, clearly defined the rating standards of security incidents and vulnerabilities and the corresponding handling procedures, and established a dedicated Security Advisory and Security Notice page. We have also established a dedicated security emergency response team to implement security contingency plans, loss reduction, analysis, locating, and remediation, and to perform backtracking/countering operations with related departments in accordance with security incident handling regulations and requirements.* (HUAWEI, 2022b)

- **Does the privacy policy specify how data is stored?** Yes, through a set of vague statements that do not specify how or where the data is, in fact, stored.

e. Information stored in the cloud. For example, the information you upload to the cloud will be stored on our servers for rapid access and sharing between devices. No one has access to such information without your permission.
Personal data collected and generated during our operations in the People's Republic of China will be stored in China. If specific products/services involve cross-border transfer of personal data, we will provide personal data to the receiving party outside China after fulfilling legal obligations (for example, after passing regulatory security assessment).

(HUAWEI, 2022b)

- **Does the privacy policy mentioned agree with current law?** The Privacy Policy states that local laws depending on the region may apply, but doesn't expand on any specific regulations. On the Children's Privacy Policy, there are no mentions of any children related laws.
- **Does the policy mention access for minors' deity?** Could not determine.
- **Does the policy address privacy issues related to children?** Huawei provides a Huawei Consumer Business Statement About Children's Privacy Protection[35] though it contains a rather lean set of statements.
- **Does the policy clearly explain what happens to the user's data if he deletes the account?** No.

For the **Rights of the Data Subject** category, Huawei barely provides enough information to the user in regards of their rights under any international regulations and does not go out of its way to inform ways that users can get in contact with the company.

- **Is the user free to access data about yourself even stored by application?** Could not determine.
- **Does the privacy policy specify the user rights?** Yes. There is more information available regarding state privacy laws on the main Huawei Privacy Policy page, but the statements are vague.

  Legislation in certain countries and regions where we provide products and services stipulates that data subjects have rights to access, correct, and delete personal data, and restrict personal data processing. According to local laws, personal data subjects or their agents can submit requests for exercising data subjects' rights (referred to as "requests") to us.

  (1) Requesting methods and channels
  Data subjects' requests must be submitted in writing. The requests are equally valid even if the requester does not specify the laws on which the requests are based. In general, verbal requests are not valid unless otherwise permitted by local laws.
  Data subjects' requests can be submitted through the official website of Huawei Consumer BG, My HUAWEI app, or HUAWEI ID Privacy centre. If a data subject initiates a request via a hotline, email, online customer service, service centre, or other channels, we will

[35] Huawei Consumer Business Statement About Children's Privacy Protection - Huawei <https://consumer.huawei.com/minisite/legal/childprivacy/statement.htm?code=CN&language=en-GB>

instruct the data subject to raise an official request through one of the aforementioned channels to facilitate progress communication and result feedback. We have established the dedicated channels to protect their legitimate interests, ensure our business operation, and prevent their rights from being misused or fraudulently used. (HUAWEI, 2022b)

- **Does the privacy policy report data to contact the company?** The main Privacy Policy page has no direct links or contacts. It guides the user to seek a Contact Us page, which can be found at the footer of the website. There are no contact information in the Children's privacy policy either.

When it comes to the **Changes to the Privacy Policy** category, Huawei indirectly transfers responsibility over to the user for checking their privacy policy updates while simultaneously failing to mention any other measures taken to assure that the changes reach the user.

- **How are changes in policies handled?** Huawei only discloses the following regarding changes to the privacy policy: *Huawei reserves the right to update this Statement at any time. This Statement may be updated from time to time. For the latest version, please visit our official website (https://consumer.huawei.com). If major changes are made to this Statement, we may notify you through different channels, for example, posting a notice on our website or sending you direct notification.* (HUAWEI, 2022b) No such thing is addressed in the Children's privacy policy.
- **What effect a change of privacy policy to an application imposes on the user?** No further information is provided.
- **How is the frequency of modification of the policy privacy?** The last modification to the main Huawei privacy policy is dated 30 July 2022 on the official website. No version history is available.

The aspects of the **User Consent and Permission** category were covered based on the information provided by the privacy policy alone as we did not assess the application for the device.

- **What is the method of choosing the user for consent or not with the policy of privacy?** Could not determine.
- **Does the user have the option of not agreeing with the applicable privacy policy?** The Children's privacy policy does not mention anything in regards to either refusing or revoking consent.
- **Is the user allowed to select what information it allows to be collected?** Could not determine.

A.4 Privacy Policy Quality Criteria Catalogue

The table below describes the original quality criteria catalogue proposed by Terra et al. (TERRA; VILELA; PEIXOTO, 2022):

Category	**Criteria**	**Description**
User Experience	Does the application present the Privacy Policy when the useraccesses the platform?	For these criteria, it is necessary to assess whetherthe user can access the Privacy Policy via anexternal link or a popup as soon as he enters the application.
	How easy is it for the user to findthe Privacy Policy in the App?	The location where the link to the Privacy Policyis allocated and what visibility from him to the user.
	Is the document adequately translated to all the languages that the application supports?	The application privacy must be correctly written and translated to all languages that the application gives support.
	Is the Privacy Policy accessible to people with disabilities (PWD)?	The document text must present visual adjustments, like increasing and decreasing the text font or adjusting colors to aid users with low vision reading.
	Does the document present a readability level compatible with what the application users can read?	The Privacy Policy needs to be read and understood by users of the application; it must not be a long and tedious read. You should avoid the use of technical terms.
	Is the document responsive?	It is necessary that the Privacy Policy be available on devices with different screen sizes, whether desktop or mobile.
	Does the document present good usability in devices with different screen sizes?	The user experience of reading the Privacy Policy must be good, even on mobile devices.

Privacy Policy Content	Is the Privacy Policy based on the assumption that the visit to the application implies the user's consent to the Policy, independent of the user reading the document or not?	It is necessary that the user actively confirm that is in accordance with the practices of application data collection; it is not enough to consider that the user confirms terms of use if he only uses the application.
	Does the policy specify clearly what data is collected?	It is important that the Policy privacy detail clearly what data will be collected by the application.
	Does the Privacy Policy specify clearly how the data is collected?	The Policy needs to express clearly which tools the application used to collect data.
	Does the Privacy Policy clearly specify if the application does use some tool or external service?	If any external services are used, it is necessary to have a link to the Privacy Policy of this third tool.
	Does the Privacy Policy specify how the company can use the collected data?	The Policy must indicate which purpose of collecting users' information.
	Does the Privacy Policy specify whether the information can be shared or sold to third parties?	If it involves third parties, it is necessary to describe that type of information that is shared, who the third parties are, and how the third parties can be classified and attached to the Privacy Policy of this third company.
	Does the Privacy Policy specify whether the data supply requested is voluntary or mandatory and the consequences of refusing to provide the requested information?	This criterion seeks to assess whether the Privacy Policy is flexible. that is, what happens if the user chooses not to provide certain information. For example, there are applications that use various tools of a smartphone such as microphone, GPS, and access to the list of contacts.

	Does the privacy policy specify the measures adopted by the application to ensure the confidentiality, integrity, and quality of Dice?	This criterion seeks to assess whether the application has some method to ensure the confidentiality and data integrity of the user. For example, if the data storage is encrypted or some IP mask is used.
	Does the privacy policy specify how data is stored?	They are informing how the data the company is stored spends more considerable credibility for your users.
	Does the privacy policy mentioned agree with current law?	The policy must bring explicitly if you are according to some law of privacy and indicate which law this is.
	Does the policy mention access for minors' deity?	If the application allows access to minors of age, the privacy policy must address this topic.
	Does the policy address privacy issues related to children?	It is necessary to explain clearly how they raise questions related to privacy with children who access the application.
	Does the policy clearly explain what happens to the user's data if he deletes the account?	It is important that the policy describe what happens if the user unlinks from the application in the policy.
Rights of the data subject	Is the user free to access data about yourself even stored by application?	It is good practice to allow the user to view the data stored by the application. So, users may dispute the accuracy and the integrity of that data.

	Does the privacy policy specify the user rights?	The privacy laws have rights that users have. It is good practice that policy describes these rights regarding personal data.
	Does the privacy policy report data to contact the company?	Ideally, there should be company area contact dealing with data privacy issues of your users.
Changes to the Privacy Policy	How are changes in policies handled?	After any change in the privacy policy, the users need to be informed and notified.
	What effect a change of privacy policy to an application imposes on the user?	Are users induced to read the new version of the policy of privacy? A good one practice is when the user enters the application it be redirected to a page clearly demonstrating the comparison between the versions.
	How is the frequency of modification of the policy privacy?	Constant changes in privacy policy do cause the company to lose user credibility.
User Consent and Permission	What is the method of choosing the user for consent or not with the policy of privacy?	The user must mark actively that is in accordance with the policy of Application privacy. Like in an opt-in format, for example.
	Does the user have the option of not agreeing with the applicable privacy policy?	The application must address the fact that the user possibly disagrees with the Privacy Policy.
	Is the user allowed to select what information it allows to be collected?	It is good practice that the user selects which information allows being collected and that the application handles each case the user does not accept that certain information is collected.

A.5 Resources for Questionnaire Directives

- **General Data Protection Regulation (GDPR)**
  - **Art. 4 – GDPR**
  - **Art. 5 – GDPR**

  - **Art. 7 – GDPR**
  - **Art. 8 – GDPR**
  - **Art. 18 – GDPR**
  - **Chapter 3 – GDPR**
  - **Chapter 4 – GDPR**
  - **Recital 35 – GDPR**
  - **Right to be Informed – GDPR**

- **The Personal Information Protection and Electronic Documents Act (PIPEDA)**
- **California Consumer Privacy Act (CCPA)**
- **California Online Privacy Protection Act (CalOPPA)**
- **Children's Privacy** – Federal Trade Commission (FTC)[36]
  - *The Children's Online Privacy Protection Act (COPPA) gives parents control over what information websites can collect from their kids. The COPPA Rule puts additional protections in place and streamlines other procedures that companies covered by the rule need to follow. The COPPA FAQs can help keep your company COPPA compliant. Learn about the COPPA Safe Harbor Program and about organizations the FTC has approved to implement safe harbor programs. You can also get information about ways to get verifiable parental consent– including new methods the Commission has approved – and the process for seeking approval for new methods.*
- **Children's Online Privacy Protection Rule ("COPPA")** – Federal Trade Commission (FTC)
  - *COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.*
- **Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business** – Federal Trade Commission (FTC)
  - *"When it comes to the collection of personal information from children under 13, the Children's Online Privacy Protection Act (COPPA) puts parents in control. The Federal Trade Commission, the nation's consumer protection agency, enforces the COPPA Rule, which spells out what operators of websites and online services must do to protect children's privacy and safety online. Here's a step-by-step plan for*

[36] Federal Trade Commission (FTC) <https://www.ftc.gov/>

determining if your company is covered by COPPA — and what to do to comply with the Rule."

- **Complying with COPPA: Frequently Asked Questions** – Federal Trade Commission (FTC)
  - *The following FAQs are intended to supplement the compliance materials available on the FTC website. This document serves as a small entity compliance guide pursuant to the Small Business Regulatory Enforcement Fairness Act.*
- **COPPA Safe Harbor Program** – Federal Trade Commission (FTC)
  - *The Children's Online Privacy Protection Act (COPPA) includes a provision enabling industry groups or others to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule. The COPPA requires the Commission to act on a request for "safe harbor" treatment within 180 days of the filing of the request, and after the proposed guidelines have been subject to notice and comment.*

    List of currently approved Safe Harbor organizations:

    * Children's Advertising Review Unit (CARU)[37]
    * Entertainment Software Rating Board (ESRB)[38]
    * iKeepSafe[39]
    * kidSAFE[40]
    * Privacy Vaults Online, Inc. (d/b/a PRIVO)[41]
    * TRUSTe[42]

[37] CARU – BBB Programs <https://caru.bbbprograms.org/>
[38] Entertainment Software Rating Board (ESRB) <https://www.esrb.org/>
[39] iKeepSafe - COPPA Certified Products <https://ikeepsafe.org/products/#coppa>
[40] kidSAFE Seal Program <https://www.kidsafeseal.com/aboutourprogram.html>
[41] PRIVO <https://www.privo.com/home>
[42] TRUSTe – Privacy Certification Standards <https://trustarc.com/consumer-information/privacy-certification-standards/>

B Attachments

B.1 Privacy Policy Quality Criteria Catalogue

The table below describes the original quality criteria catalogue proposed by Terra et al. (TERRA; VILELA; PEIXOTO, 2022):

Category	**Criteria**	**Description**
User Experience	Does the application present the Privacy Policy when the useraccesses the platform?	For these criteria, it is necessary to assess whetherthe user can access the Privacy Policy via anexternal link or a popup as soon as he enters the application.
	How easy is it for the user to findthe Privacy Policy in the App?	The location where the link to the Privacy Policyis allocated and what visibility from him to the user.
	Is the document adequately translated to all the languages that the application supports?	The application privacy must be correctly written and translated to all languages that the application gives support.
	Is the Privacy Policy accessible to people with disabilities (PWD)?	The document text must present visual adjustments, like increasing and decreasing the text font or adjusting colors to aid users with low vision reading.
	Does the document present a readability level compatible with what the application users can read?	The Privacy Policy needs to be read and understood by users of the application; it must not be a long and tedious read. You should avoid the use of technical terms.
	Is the document responsive?	It is necessary that the Privacy Policy be available on devices with different screen sizes, whether desktop or mobile.
	Does the document present good usability in devices with different screen sizes?	The user experience of reading the Privacy Policy must be good, even on mobile devices.

Privacy Policy Content	Is the Privacy Policy based on the assumption that the visit to the application implies the user's consent to the Policy, independent of the user reading the document or not?	It is necessary that the user actively confirm that is in accordance with the practices of application data collection; it is not enough to consider that the user confirms terms of use if he only uses the application.
	Does the policy specify clearly what data is collected?	It is important that the Policy privacy detail clearly what data will be collected by the application.
	Does the Privacy Policy specify clearly how the data is collected?	The Policy needs to express clearly which tools the application used to collect data.
	Does the Privacy Policy clearly specify if the application does use some tool or external service?	If any external services are used, it is necessary to have a link to the Privacy Policy of this third tool.
	Does the Privacy Policy specify how the company can use the collected data?	The Policy must indicate which purpose of collecting users' information.
	Does the Privacy Policy specify whether the information can be shared or sold to third parties?	If it involves third parties, it is necessary to describe that type of information that is shared, who the third parties are, and how the third parties can be classified and attached to the Privacy Policy of this third company.
	Does the Privacy Policy specify whether the data supply requested is voluntary or mandatory and the consequences of refusing to provide the requested information?	This criterion seeks to assess whether the Privacy Policy is flexible. that is, what happens if the user chooses not to provide certain information. For example, there are applications that use various tools of a smartphone such as microphone, GPS, and access to the list of contacts.

	Does the privacy policy specify the measures adopted by the application to ensure the confidentiality, integrity, and quality of Dice?	This criterion seeks to assess whether the application has some method to ensure the confidentiality and data integrity of the user. For example, if the data storage is encrypted or some IP mask is used.
	Does the privacy policy specify how data is stored?	They are informing how the data the company is stored spends more considerable credibility for your users.
	Does the privacy policy mentioned agree with current law?	The policy must bring explicitly if you are according to some law of privacy and indicate which law this is.
	Does the policy mention access for minors' deity?	If the application allows access to minors of age, the privacy policy must address this topic.
	Does the policy address privacy issues related to children?	It is necessary to explain clearly how they raise questions related to privacy with children who access the application.
	Does the policy clearly explain what happens to the user's data if he deletes the account?	It is important that the policy describe what happens if the user unlinks from the application in the policy.
Rights of the data subject	Is the user free to access data about yourself even stored by application?	It is good practice to allow the user to view the data stored by the application. So, users may dispute the accuracy and the integrity of that data.

	Does the privacy policy specify the user rights?	The privacy laws have rights that users have. It is good practice that policy describes these rights regarding personal data.
	Does the privacy policy report data to contact the company?	Ideally, there should be company area contact dealing with data privacy issues of your users.
Changes to the Privacy Policy	How are changes in policies handled?	After any change in the privacy policy, the users need to be informed and notified.
	What effect a change of privacy policy to an application imposes on the user?	Are users induced to read the new version of the policy of privacy? A good one practice is when the user enters the application it be redirected to a page clearly demonstrating the comparison between the versions.
	How is the frequency of modification of the policy privacy?	Constant changes in privacy policy do cause the company to lose user credibility.
User Consent and Permission	What is the method of choosing the user for consent or not with the policy of privacy?	The user must mark actively that is in accordance with the policy of Application privacy. Like in an opt-in format, for example.
	Does the user have the option of not agreeing with the applicable privacy policy?	The application must address the fact that the user possibly disagrees with the Privacy Policy.
	Is the user allowed to select what information it allows to be collected?	It is good practice that the user selects which information allows being collected and that the application handles each case the user does not accept that certain information is collected.

Bibliography

ANAYA, L. H. S. et al. Ethical implications of user perceptions of wearable devices. Science and Engineering Ethics, v. 24, p. 1–28, 02 2017. Cited on page 13.

ANGULO, J. et al. Towards usable privacy policy display and management. Information Management Computer Security, v. 20, p. 4–17, 03 2012. Cited on page 61.

AYALA-RIVERA, V.; PASQUALE, L. The grace period has ended: An approach to operationalize gdpr requirements. 2018 IEEE 26th International Requirements Engineering Conference (RE), 08 2018. Cited 2 times on pages 16 and 27.

BECHER, S. I.; BENOLIEL, U. Law in books and law in action: The readability of privacy policies and the gdpr. Consumer Law and Economics, p. 179–204, 09 2020. Cited 2 times on pages 19 and 20.

BLOOMBERG, L. D. Completing Your Qualitative Dissertation. 2019. Disponível em: <https://us.sagepub.com/en-us/nam/completing-your-qualitative-dissertation/book279950>. Cited on page 21.

Cavoukian, A.; Kursawe, K. Implementing privacy by design: The smart meter case. In: 2012 International Conference on Smart Grid (SGE). [S.l.: s.n.], 2012. p. 1–8. Cited on page 16.

CREASER, A. V. et al. The acceptability, feasibility, and effectiveness of wearable activity trackers for increasing physical activity in children and adolescents: A systematic review. International Journal of Environmental Research and Public Health, v. 18, p. 6211, 06 2021. Cited on page 59.

ERMAKOVA, T. et al. Privacy policies and users' trust: Does readability matter? 01 2014. Cited on page 19.

FERNáNDEZ-CARAMéS, T.; FRAGA-LAMAS, P. Towards the internet-of-smart-clothing: A review on iot wearables and garments for creating intelligent connected e-textiles. Electronics, v. 7, p. 405, 12 2018. Cited on page 13.

FIETKIEWICZ, K.; ILHAN, A. Fitness Tracking Technologies: Data Privacy Doesn't Matter? The (Un)Concerns of Users, Former Users, and Non-Users. [S.l.], 2020. Cited 3 times on pages 9, 14, and 18.

FúSTER, J. et al. Analysis of security and privacy issues in wearables for minors. Wireless Networks, 03 2023. Cited 2 times on pages 9 and 19.

GABRIELE, S.; CHIASSON, S. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 04 2020. Cited on page 62.

GENERAL DATA PROTECTION REGULATION (GDPR). Art. 8 GDPR – Conditions applicable to child's consent in relation to information society services | General Data Protection Regulation (GDPR). 2019. Disponível em: <https://gdpr-info.eu/art-8-gdpr/>. Cited on page 17.

Gürses, S.; del Alamo, J. M. Privacy engineering: Shaping an emerging field of research and practice. IEEE Security Privacy, v. 14, n. 2, p. 40–46, 2016. Cited 2 times on pages 15 and 16.

HADAR, I. et al. Privacy by designers: Software developers' privacy mindset. In: Proceedings of the 40th International Conference on Software Engineering. New York, NY, USA: Association for Computing Machinery, 2018. (ICSE '18), p. 396. ISBN 9781450356381. Disponível em: <https://doi.org/10.1145/3180155.3182531>. Cited on page 16.

HARTUNG, P. The children's rights-by-design standard for data use by tech companies. UNICEF, 2020. Disponível em: <https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf>. Cited 2 times on pages 17 and 18.

HUAWEI. Huawei Consumer Business Statement About Children's Privacy Protection. 2022. Disponível em: <https://consumer.huawei.com/minisite/legal/childprivacy/statement.htm?code=CN&language=en-GB>. Cited 5 times on pages 103, 105, 107, 108, and 109.

HUAWEI. Privacy Statement - HUAWEI Global. 2022. Disponível em: <https://consumer.huawei.com/en/privacy/privacy-policy/>. Cited 7 times on pages 104, 106, 107, 108, 109, 110, and 111.

IBDAH, D. et al. "why should i read the privacy policy, i just need the service": A study on attitudes and perceptions toward privacy policies. IEEE Access, v. 9, p. 166465–166487, 2021. Cited on page 19.

KRETSCHMER, M.; PENNEKAMP, J.; WEHRLE, K. Cookie banners and privacy policies: Measuring the impact of the gdpr on the web. ACM Transactions on the Web, v. 15, p. 1–42, 07 2021. Cited on page 20.

KRUMAY, B.; KLAR, J. Readability of privacy policies. Data and Applications Security and Privacy XXXIV, p. 388–399, 2020. Cited on page 19.

LI, Z. S. et al. GDPR Compliance in the Context of Continuous Integration. 2020. Disponível em: <https://arxiv.org/abs/2002.06830>. Cited on page 16.

LIDYNIA, C.; BRAUNER, P.; ZIEFLE, M. A Step in the Right Direction – Understanding Privacy Concerns and Perceived Sensitivity of Fitness Trackers. 2017. Disponível em: <https://www.semanticscholar.org/paper/A-Step-in-the-Right-Direction-%E2%80%93-Understanding-and-Lidynia-Brauner/6592f622892bff56643d6dfdf678dd975c88bf58>. Cited on page 62.

LIVINGSTONE, S. Children: a special case for privacy? Intermedia, v. 46, p. 18–23, 07 2018. Disponível em: <https://eprints.lse.ac.uk/89706/>. Cited on page 18.

LYALL, B. 'build a future champion': exploring a branded activity-tracking platform for children and parents. Media International Australia, p. 1329878X2110071, 04 2021. Cited on page 14.

MACKINTOSH, K. A. et al. Parental perspectives of a wearable activity tracker for children younger than 13 years: Acceptability and usability study. JMIR mHealth and uHealth, v. 7, 11 2019. Cited 2 times on pages 9 and 14.

Martin, Y.; Kung, A. Methods and tools for gdpr compliance through privacy and data protection engineering. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW). [S.l.: s.n.], 2018. p. 108–111. Cited on page 16.

MORKONDA, S. G.; CHIASSON, S.; OORSCHOT, P. C. van. Empirical analysis and privacy implications in oauth-based single sign-on systems. Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society, 11 2021. Cited on page 59.

MOZILLA. Our Methodology - *Privacy Not Included: A Buyer's Guide for Connected Products. 2022. Disponível em: <https://foundation.mozilla.org/en/privacynotincluded/about/methodology/>. Cited on page 24.

MOZILLA. Review: Huawei Watch Kids 4 Pro. 2022. Disponível em: <https://foundation.mozilla.org/en/privacynotincluded/huawei-watch-kids-4-pro/>. Cited 2 times on pages 71 and 72.

MOZILLA. Review: Spacetalk Adventurer. Mozilla, 2022. Disponível em: <https://foundation.mozilla.org/en/privacynotincluded/spacetalk-adventurer/>. Cited 2 times on pages 67 and 68.

MOZILLA. Review: Ticktalk 4. Mozilla, 2022. Disponível em: <https://foundation.mozilla.org/en/privacynotincluded/ticktalk-4/>. Cited 3 times on pages 69, 70, and 71.

MOZILLA. Review: Verizon GizmoWatch. Mozilla, 2022. Disponível em: <https://foundation.mozilla.org/en/privacynotincluded/verizon-gizmowatch/>. Cited 2 times on pages 65 and 66.

NOTARIO, N. et al. Pripare: Integrating privacy best practices into a privacy engineering methodology. 2015 IEEE Security and Privacy Workshops, 05 2015. Cited on page 15.

PEIXOTO, M. et al. Towards a catalog of privacy related concepts. 2020. Disponível em: <https://ceur-ws.org/Vol-2584/PT-paper5.pdf>. Cited on page 62.

REBELO, M. E.; VALENçA, G.; LINS, F. Power and privacy in software ecosystems: A study on data breach impact on tech giants. Requirements Engineering: Foundation for Software Quality, p. 149–164, 2021. Cited 4 times on pages 9, 16, 18, and 59.

SEQUEIRA, L. et al. Mobile and wearable technology for monitoring depressive symptoms in children and adolescents: A scoping review. Journal of Affective Disorders, v. 265, p. 314–324, 03 2020. Cited on page 13.

SIMONE, v. d. H.; LIEVENS, E. The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR. 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107660>. Cited 2 times on pages 17 and 20.

SPACETALKUS. Children's Privacy Policy. 2021. Disponível em: <https://us.spacetalkwatch.com/pages/children-s-privacy-policy>. Cited 4 times on pages 81, 83, 85, and 86.

SPACETALKUS. Privacy Policy. 2021. Disponível em: <https://us.spacetalkwatch.com/pages/privacy-policy>. Cited 6 times on pages 81, 82, 83, 84, 86, and 87.

SPIEKERMANN, S. The challenges of privacy by design. Communications of The ACM - CACM, v. 55, p. 38–40, 07 2012. Cited 2 times on pages 16 and 17.

TERRA, A.; VILELA, J.; PEIXOTO, M. A catalog of quality criteria to guide the assessment of applications' privacy policies. 2022. Disponível em: <http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER22/WER_2022_Camera_ready_paper_37.pdf>. Cited 7 times on pages 11, 25, 26, 30, 62, 112, and 118.

TICKTALK. Privacy Policy. 2022. Disponível em: <https://www.myticktalk.com/pages/policies>. Cited 11 times on pages 89, 90, 92, 93, 94, 96, 97, 98, 100, 101, and 102.

VALENçA, G. et al. Do Platforms Care About Your Child's Data? A Proposal of Legal Requirements for Children's Privacy and Protection. 2022. Disponível em: <http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER22/WER_2022_Camera_ready_paper_20.pdf>. Cited on page 17.

VELYKOIVANENKO, L. et al. Are those steps worth your privacy? Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, v. 5, p. 1–41, 12 2021. Cited on page 18.

VERIZON. Gizmo Products _ Services Privacy Policy | Verizon Privacy Policy. 2023. Disponível em: <https://www.verizon.com/about/privacy/gizmo-privacy-policy>. Cited 7 times on pages 74, 75, 76, 77, 78, 79, and 104.

VERIZON. Privacy Policy Home Page | About Verizon. 2023. Disponível em: <https://www.verizon.com/about/privacy/>. Cited 4 times on pages 76, 77, 78, and 79.

WELCH, V. et al. Use of mobile and wearable artificial intelligence in child and adolescent psychiatry: Scoping review. Journal of Medical Internet Research, v. 24, p. e33560, 03 2022. Cited on page 13.

YIN, R. K. Case Study Research and Applications. 2019. Disponível em: <https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150>. Cited on page 21.