GDPR Compliance in the Metaverse

MSc Research Project
Cyber Security

Liam O'Hagan
Student ID: 22116168

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Liam O'Hagan
Student ID:	22116168
Programme:	Cyber Security
Year:	2024
Module:	MSc Research Project
Supervisor:	Mark Monaghan
Submission Due Date:	12/08/2024
Project Title:	GDPR Compliance in the Metaverse
Word Count:	13228
Page Count:	62

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Liam O Hagan
Date:	11th August 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

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

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

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

GDPR Compliance in the Metaverse

Liam O'Hagan
22116168

Abstract

An exploration of existing research concerning the Metaverse revealed a lack of data relating to GDPR compliance by Metaverse applications. This research for this report was undertaken to address this gap by measuring the level of compliance of a sample of Metaverse applications with their GDPR obligations.

Keywords: GDPR, Compliance, Metaverse, Personal Data, Privacy.

1 Introduction

A long-time proponent of data privacy, with industry certifications in data privacy and the GDPR, I deal with privacy-related queries often in my work. Becoming increasingly aware of The Metaverse, I have, given its relative novelty as a technology, speculated as to the general level of compliance of applications in The Metaverse with data privacy regulation. This research explores and examines these levels of compliance.

A literature review has identified a number of publications that have noted privacy risks in the Metaverse. However, none of the reviewed publications have attempted to measure compliance with GDPR.

This research identifies specific Metaverse applications for examination. It establishes a method of measurement that can be applied consistently across applications. Finally, it delivers conclusions based on the results of the measurements.

The results of this research may be of interest to the controllers and processors themselves; regulators; parents and guardians; and those with an interest in the Metaverse and/or Data Privacy.

Research Question. How compliant with GDPR are applications in the Metaverse?

2 Document Structure

Contents

1 Introduction 1

2 Document Structure 2

3 Introduction To The Metaverse 4

4 Introduction To The GDPR 5
- 4.1 Lawfulness, fairness and transparency . . . 5
- 4.2 Purpose limitation . . . 5
- 4.3 Data Minimisation . . . 6
- 4.4 Accuracy . . . 6
- 4.5 Storage limitation . . . 6
- 4.6 Integrity and Confidentiality . . . 6
- 4.7 Accountability . . . 6

5 Prior Research 7
- 5.1 Introduction . . . 7
- 5.2 Privacy In a Programmed Platform . . . 7
- 5.3 Security and Privacy in The Metaverse . . . 8
- 5.4 Life, the Metaverse and Everything . . . 9
- 5.5 Privacy Concerns and Measures in Metaverse . . . 9
- 5.6 Metaverse and its Regulation . . . 9
- 5.7 Privacy of the Metaverse . . . 10
- 5.8 Trust Framework for the Metaverse . . . 10
- 5.9 Oculus Virtual Reality Applications . . . 11
- 5.10 Summary . . . 11

6 Methodology 12
- 6.1 Overview . . . 12
- 6.2 Random Sample of Apps . . . 12
- 6.3 Identifying personal data processed by Apps . . . 12
- 6.4 Definition of compliance . . . 13
- 6.5 Meta Requirements . . . 14
- 6.6 Method for Measuring Compliance . . . 14
  - 6.6.1 GDPR Requirements . . . 14
  - 6.6.2 Scoring Compliance . . . 16

7 Analysis and Conclusions 17
- 7.1 Analysis of App-Related Data . . . 17
- 7.2 Analysis of Privacy Policies . . . 23
- 7.3 Conclusion . . . 28
- 7.4 Future Work . . . 30

8 Appendix 31
- 8.1 Meta Data Collection . . . 31

8.1.1 Conclusion . . . 32
8.2 Apps Selected for Assessment . . . 33
8.3 Data Collected by Apps . . . 35
8.4 Privacy Policy Analysis . . . 37
8.5 Privacy Policy Observations . . . 41

List of Tables

1 Compliance Scoring . . . 16
2 PEGI Ratings . . . 19
3 Analysis of Data Items Collected . . . 20
4 Analysis of Compliance values . . . 24
5 Apps selected for assessment . . . 33
6 Data items collected by Apps . . . 35
7 Key . . . 36
8 Privacy Policy Analysis . . . 37
9 Key . . . 40
10 Privacy Policy Observations . . . 41

List of Figures

1 Data Collected by App . . . 13
2 Categories of App . . . 17
3 Genres of App . . . 18
4 PEGI Ratings . . . 19
5 Number of data items collected . . . 20
6 User data collected . . . 21
7 Device and Sensor data collected . . . 22
8 All Apps . . . 23
9 Apps that process data . . . 23
10 Compliance Density Plot . . . 24
11 EU Membership and App Compliance . . . 25
12 Controller Location . . . 26
13 Popularity vs Compliance . . . 27

3 Introduction To The Metaverse

The word "Metaverse" is a portmanteau of "Meta", meaning "more than" or "transcending" and "verse", a shortening of "universe". The naming and the concept of a Metaverse were first introduced by author Neal Stephenson in his 1992 novel, "Snow Crash" [1]. In his novel, Stephenson describes an immersive, computer-generated world in which digital users interact with each other and their virtual environment.

In their announcement of Facebook's change of name to "Meta" [2], CEO Mark Zuckerburg's description of Meta's vision of The Metaverse as an immersive experience in which users interact with each other outside of the physical world seems difficult to differentiate from that of Stephenson's digital world.

In its "Guidelines on Data Protection Impact Assessment" (DPIA) [3], the European Data Protection Board (EDPB) acknowledged, as far back as 2017, that consequences to society and individuals associated with the use of new technologies are difficult to anticipate and that there may be a potential for high risk to the rights and freedoms of data subjects .

Although the EDPB does not identify specific risks that new technologies can introduce, it is likely that they would be not dissimilar to the current risks that data subjects face: data breach through poor safeguarding of data, misuse of personal data, over-retention, lack of consent or proper legal basis and others.

Meta (formerly Facebook) has been identified as the primary focus of this research because of its size and consequent influence on technologies that it is developing in addition to the expressed desire of Meta's CEO, Mark Zuckerberg, that Meta be viewed in relation to its Metaverse work rather than its social media work [4].

4 Introduction To The GDPR

The General Data Protection Regulation [5] was adopted in 2016 and began to be enforced from May 25th 2018. The seven principles [6] of The GDPR are

1. lawfulness, fairness and transparency
2. purpose limitation
3. data minimisation
4. accuracy
5. storage limitation
6. integrity and confidentiality
7. accountability

4.1 Lawfulness, fairness and transparency

All processing of personal data must be lawful. It must have a "Legal Basis". The six legal bases [7] are

1. Consent
2. Performance of a contract
3. Legal obligation
4. Vital interests
5. Public interest
6. Legitimate interests

The processing of personal data must be carried out in a fair and transparent manner. Those persons whose data is being processed should be made aware that their data is being processed, the reasons for the processing and in what way the data is being processed.

To support this fair processing of personal data, the controller should provide the data subject with information about the processing in an accessible and understandable way including the legal basis or bases for the processing.

In the context of processing data in The Metaverse, there are only three legal bases that can apply.

1. Consent
2. Performance of a contract
3. Legitimate Interest

It is entirely plausible for more than one legal basis to apply.

4.2 Purpose limitation

The principle of Purpose Limitation dictates that data may only be processed for the purposes for which it was collected - those purposes being specific and legal.

4.3 Data Minimisation

Data Minimisation limits the collection of data to that which is necessary for the purposes for which it is collected.

4.4 Accuracy

Personal Data should be kept accurate and up to date. Inaccurate data should be rectified as soon as possible.

4.5 Storage limitation

Personal Data may only be retained for that period which is necessary to accomplish the purposes for which it was collected.

4.6 Integrity and Confidentiality

The Controller should ensure that personal data is secured against Data Breach through the use of appropriate ”technical and organisational methods”.

A Data Breach [8] has occurred when Personal Data has been accidentally or unlawfully accessed, modified, deleted, lost or disclosed.

4.7 Accountability

The Controller must be able to demonstrate compliance with the previous principles.

5 Prior Research

5.1 Introduction

The purpose of this literature review is to establish what, if any, attempts have been made to measure GDPR compliance in the Metaverse. Of use also will be any privacy risks identified in reviewed literature.

5.2 Privacy In a Programmed Platform

Privacy In a Programmed Platform:How the General Data Protection Regulation applies to the Metaverse

In his article in “The Harvard Journal of Law & Technology”, Martin contends that the Metaverse is unlike other social media technologies and that current legislation may be insufficient to regulate the Metaverse. [9]

He notes a 2020 report that Facebook generated four Petabytes of data daily and predicts that the Metaverse will generate even more data with the potential for very sensitive data to be inferred from users' activities such as gender, ethnicity, sexual preferences, and others. These fall into the GDPR's “Special Category Data” which require additional protections.

He also observes that, of the many Facebook patents that were examined by Business Insider, not one contained a mention of privacy or safety while, at the same time, Facebook claimed to be investigating how it can reduce its use of, and grant greater control to data subjects over, their personal data.

The article identifies the collection of biometric data as enabling more “invasive” targeting of users for and by advertisers.

Martin's article does contain what appears to be a significant factual inaccuracy. The article states that “Based on Recital 23 of the GDPR, which provides supporting context for Article 3 on the material scope of the regulation, foreign companies are only required to comply with the GDPR if they target EU residents with their marketing.”

This claim appears to directly contradict the sentence immediately prior to the claim, in which Martin notes that non-EU entities must comply with GDPR if it offers “virtual goods and service” to users in the EU.

In fact, neither Article 3 nor Recital 23 mention marketing at all. Article 3 clearly states that the processing of the data of data subjects in the union in relation to the offering of goods and services is within the territorial scope of the GDPR. Recitals 22 to 24 add additional context but do not support Martin's claim.

As Martin attempts to make a case that GDPR is insufficient to regulate the Metaverse, this inaccuracy may weaken his case.

The article advocates for strong age-verification controls and the requirement for explicit consent in relation to advertising in the Metaverse. However, it has not been made clear that there is a gap or weakness in the current regulations.

Martin argues that the Metaverse should not be subject to the GDPR's data transfer controls. This is to “facilitate functionality and interoperability”. However, Martin does not explain how the removal of data transfer obligations will aid functionality and interoperability. Nor does he explore the risks of such removal.

The article inaccurately describes personal data by as including data “that does not directly identify a named person if it could still help identify the “data subject.”” In fact, Article 4 of the GDPR defines personal data as “any information relating to an identified or identifiable natural person”. Whether or not the data being considered assists in identifying the data subject is not a factor. This may appear like a minor distinction between. However, it directly impacts the scope of data covered by the GDPR so is not insignificant.

Martin does make an important point in relation to the storage of information in a blockchain. The immutable nature of blockchain data does appear to be in conflict with the data subject’s “right to be forgotten”. He incorrectly concludes that this conflict renders moot the right to be forgotten. The conflict may, however, need to be resolved in some way.

The article concludes that the GDPR needs to adapt alongside the Metaverse. However, Martin has not identified any conclusive shortcomings in the GDPR. I believe that Martin’s discussion of the Metaverse and the GDPR does make a useful contribution. However, I disagree with a number of points that he makes in his article including his conclusion.

5.3 Security and Privacy in The Metaverse

Security and Privacy in The Metaverse: A Comprehensive Survey

In their article, Y. Wang et al. report their results of a survey of the Metaverse with a focus on security and privacy [10].

Y. Wang et al. discuss some risks to which new technologies are susceptible and, having cited examples of categories of recent compromises of new technologies, they reason that it is not a big leap to the compromise of a physical device used to access the metaverse and, from there, to risks to personal safety and even Critical National Infrastructure.

They note that Metaverse users may be subject to the increased collection of biometric data by the use of augmented/virtual reality headsets. In order for the user and the Metaverse to interact, the collection of very detailed information such as eye and hand movements, brain waves and facial expressions may be required.

The increased volumes of collected data pose an elevated risk should the data suffer unauthorised access. Wang et al suggest a number of Data Leakage scenarios including the transmission, processing and storage of data. They also identify a privacy risk resulting from the linkage of data between platforms.

They also suggest mitigations in relation to User Generated Content (UGC) and digital footprints.

At two points, the authors refer to personal data collected as PII (Personally Identifiable Information). This is primarily an American term. Personal data, as defined in the GDPR has a far greater scope. However, the use of this term does not appear to have limited the authors’ view on the scope of data to be protected. It may simply be the use of a familiar term to mean personal data.

The report observes that Meta has introduced an age-certification mechanism in 2021. On the surface, this may address the concerns raised by Martin in the previous section in relation to strong age verification control requirements.

The article identifies goes into some technical detail about the Metaverse architecture and identifies a number of security concerns along with some countermeasures. However, I did not identify any measurement of compliance with privacy regulations.

5.4 Life, the Metaverse and Everything

Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse

In addition to an ethical examination of the Metaverse, Hui and Fernandez explore privacy and governance in the Metaverse. [11]

The authors, as in the earlier reviewed documents, identify the collection of biometric data as a risk.

They also pose an example of sexual harassment as a risk. While this does seem, to this researcher, to be a valid concern, the broadening of this example to include a possible killing of one avatar by another does seem somewhat unrealistic.

They discuss the imposition of rules and codes and raise an interesting question about how local rules can be applied to a global Metaverse. However, they only mention GDPR in passing and there is no attempt to measure compliance.

5.5 Privacy Concerns and Measures in Metaverse

Privacy Concerns and Measures in Metaverse: A Review

Much like the previous documents, Canbay et al discuss privacy issues raised by the Metaverse and present some measures to address these privacy issues. [12]

However, this document was the first reviewed to identify comprehensive and specific details about the personal data being gathered in and by the Metaverse. Whilst previous documents identified categories of data with some specifics, the authors identify many interesting specific types of personal data including facial expressions, brainwaves, feelings, habits, and digital assets.

They make an interesting point in relation to a potential incompatibility of privacy regulations between the Metaverse and the real world and propose the creation of Metaverse-compatible privacy regulation. They also identify incompatibilities between different privacy frameworks such as GDPR, UK privacy laws and Turkish data protection laws. They then call for the elimination of these inconsistencies in the Metaverse.

The authors propose a number of measures for address some of the privacy concerns that they have identified. However, no discussion of the levels of compliance takes place.

5.6 Metaverse and its Regulation

Metaverse and its Regulation

The author conducts a literature review of material sourced in legal databases and other sources. [13]

This is an excellent paper that appears to take no particular position, but which reports objectively on reviewed material. Aamir is clear that an agreed definition of the Metaverse remains elusive but quotes a definition by Jooyoung Kim that attempts to cohere elements of other definitions. He describes the Metaverse as “an interoperated persistent network of shared virtual environments where people can interact synchronously through their avatars with other agents and objects” [14].

Aamir echoes a point made in other papers in this review that regulation in the Metaverse may prove difficult in that the global nature of the Metaverse makes the imposition of any single regulatory framework problematic.

The author also repeats the inconsistency mentioned by an earlier paper in relation to the immutability of blockchain data and the GDPR’s “right to be forgotten”.

5.7 Privacy of the Metaverse

Privacy of the Metaverse: Current Issues, AI Attacks, and Possible Solutions

In this paper [15], the authors identify 6G networks and new technologies that will be the enablers of the Metaverse.

This is an interesting paper that identifies privacy threats from technologies that are as yet unavailable in the Metaverse.

While it does suggest some mitigation such as Privacy by Design and Encryption - both recommended by GDPR - and it does suggest GDPR as a consideration, the measurement of GDPR compliance of individual Apps is not a consideration.

5.8 Trust Framework for the Metaverse

Security Risks, User Privacy Risks, and a Trust Framework for the Metaverse Space

Kharvi introduces [16] an interesting concept of an overarching trust factor in relation to Metaverse applications. The four elements of the trust factor are Security, Privacy, Availability and Recovery. From the point of view of Data Privacy, the first two elements are of interest.

The author proposes that all Metaverse applications undergo a trust assessment (and automated, ongoing assessments) prior to on-boarding. The assessment consists of specific checks in relation to Security and Privacy such as transparency of disclosure of policies and procedures and the processes for handling personal data.

An overall trust score is an interesting, consumer-friendly way to communicate an App’s compliance with Meta’s own privacy policies and, perhaps, international standards. The automation of such an assessment would require a significant departure from the current method of simply publishing a link to the developer’s privacy policy.

5.9 Oculus Virtual Reality Applications

An Empirical Study on Oculus Virtual Reality Applications: Security and Privacy Perspectives

Although this paper [17] is included in ”Prior Research”, it was encountered towards the end of the preparation of this report. The paper was published in IEEE Explore in June 2024 so was not available during the initial research period. However, the paper has a significant overlap with this report’s objective, hence its inclusion.

The authors in this paper adopted a unique approach in that they created a tool to decompile a Meta Quest App and perform a static code analysis on the decompiled APK (Android Package Kit). The tool also analyses the privacy policy for the app. The authors performed this analysis on 500 apps. Significantly, the tool attempts to detect Privacy Policy compliance with GDPR (the objective of this report).

The results of the GDPR Compliance check in the paper are not quite consistent with those of this report. Both do identify significant levels of non-compliance. However, this report is less strict and has adopted a 75% compliance level as being ”generally compliant”.

Additionally, this report relies entirely on the contents of the Privacy Policy for analysis. The paper’s authors compare the Privacy Policy to the ***actual*** data usage in the application.

There is, however, some room for error in this approach. If the data is being processed entirely on the device and is not communicated to the developer or any other party, then this researcher would not consider this to be the processing of personal data. The Privacy Policy has no requirement, therefore, to meet any GDPR requirements in its Privacy Policy.

This is an important paper that made for very interesting reading.

5.10 Summary

The documents reviewed agree that the Metaverse presents new risks to privacy. There appears to be consensus that the Metaverse brings new privacy risks and that additional, or perhaps specific, regulation is required to protect the rights of data subjects in the Metaverse.

At the time of initial research, none of the papers reviewed contained any information on compliance levels with the GDPR or other privacy framework.

However, towards the end of this report’s preparation, a newly published paper reports on an automated GDPR compliance check of Apps’ Privacy Policies.

As the Metaverse’s reach expands and the number of applications grow, it is expected that public and regulators’ interest in this technology will increase correspondingly. Reports such as this and the ”Oculus Virtual Reality Applications” study [17] may be of some use to both.

6 Methodology

6.1 Overview

Data was collected from a random sample of Meta Apps in the Meta Quest app Store [18] for evaluating compliance with the GDPR [5].

The collection and evaluation consists of

1. Identifying a random sample of Apps
2. Identifying data processed by Apps
3. Establishing a definition of compliance
4. Establishing a method for measuring compliance
5. Evaluating each App in the sample for compliance
6. Reporting on the results of the evaluation

6.2 Random Sample of Apps

It is understood that unofficial apps are available from sources other than Meta. For the purposes of this research, only official Apps from the Meta Quest App Store have been considered.

No official, definitive listing of available Meta Quest Apps was available. Accordingly, data from the Meta Quest App Store was manually downloaded, cleaned, sorted and de-duplicated. This resulted in a list of 644 unique applications from which 65 apps were randomly selected.

6.3 Identifying personal data processed by Apps

Personal data may be collected [19] directly by the App through the Meta Quest headset and handheld controllers. Personal data may, additionally, be collected by the App from Meta via the user's account with Meta. Finally, personal data may be collected by the App Developer directly through the creation of, and interaction with, an account with the developer.

There are two categories of data collected by the Quest headset and controllers:

1. Sensor and device data
2. Your information

Sensor and Device Data (from device)

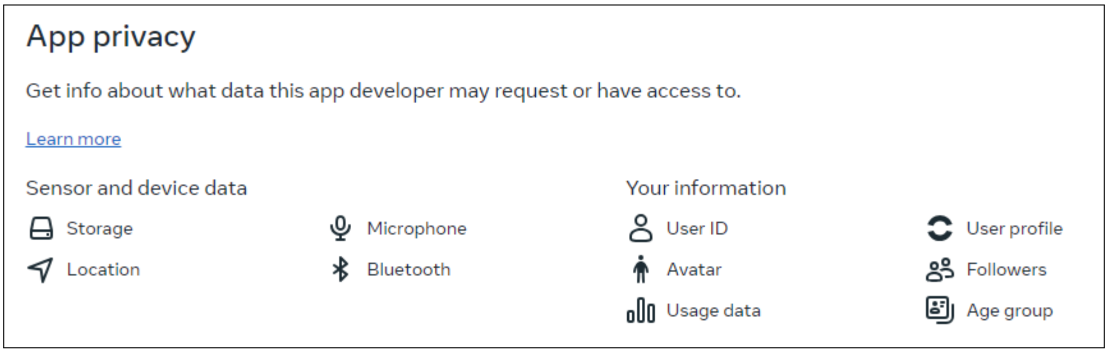
- Microphone
- Storage
- Location
- Bluetooth

- Spatial Data
- Hand Tracking
- Eye Tracking

Your Information (from Meta)

- User ID
- User Profile
- Avatar
- Followers
- Usage Data
- Age Group

The data collected by the device for each App is identified on the App’s web page in the Meta Quest App Store. This is an example (from an App’s web page in the App Store) of the data that an App has access to.



App privacy

Get info about what data this app developer may request or have access to.

Learn more

Sensor and device data

Storage

Microphone

Location

Bluetooth

Your information

User ID

User profile

Avatar

Followers

Usage data

Age group

Figure 1: Data Collected by App

For each App in the random sample, the data identified in the App’s web page is recorded against that App.

6.4 Definition of compliance

For the purpose of this report, a binary measure of compliance - where an App is either entirely compliant or not - is considered to have less value than a measure of the ***level*** of compliance.

A ***level*** of compliance allows for the selection of a value beyond which an App may be considered to be ”generally compliant”.

The value chosen for this report is 75%. That is, Apps that are scored at a compliance level of 75% or greater will be considered to be ”generally compliant” with The GDPR.

6.5 Meta Requirements

Meta requires that the App developer's use of personal data complies with Meta's Developer Data Use Policy [20]. Further, it identifies Privacy Policy Requirements [21] which with the developer must also comply.

There are a number of requirements in common between Meta and The GDPR. This report does not attempt to measure compliance with Meta's policies.

The presence of Meta's obligations on the developer is noted as an effort on Meta's part to ensure compliance of its platform and hosted Apps with The GDPR.

6.6 Method for Measuring Compliance

6.6.1 GDPR Requirements

The GDPR places specific requirements on controllers and processors in relation to the provision of information to data subjects whose data is being processed.

In order to establish the role of the developer in the processing of personal data, it is necessary to refer to The GDPR's definitions.

Is the app developer a controller or a processor?

Article 4 [8] defines a processor as one who processes personal data on behalf of a controller. Article 28 [22] requires that a processor processes data under contract with the controller and identifies the nature and details of the contract.

App developers do not process the user's data ***on behalf*** of Meta. Rather, the developer may collect the user's data directly via the creation of an account with the developer. Additionally, the developer collects and uses the user's data in the context of the operation of the App.

No evidence has been discovered of any data processing contractual arrangement between Meta and its developers.

Accordingly, in the context of GDPR, it has been concluded that developers are controllers.

Is the app developer a joint controller?

Article 26 [23] defines Joint Controllers as those who ***jointly*** determine the purposes and means of processing. They must transparently determine their respective responsibilities in relation to compliance with The GDPR.

No evidence of any arrangement between Meta and developers has been discovered to suggest that any such arrangement is in place. Developers have, accordingly, been concluded to controllers in their own right.

Controllers' obligations in relation to provision of information

In The GDPR, Articles 12 [24], 13 [25] and 14 [26] identify the information that must be provided to Data Subjects in relation to the processing of their personal information.

Article 12 [24] requires that the Data Subject is provided with information relating to the processing of their information in a clear and transparent manner. The information should be easily accessible. Where the reader is expected to be a child, the language used should be clear and plain.

This article also places an obligation on the controller to accommodate requests from a Data Subject in relation to their rights.

Article 13 [25] identifies the information that a controller **must** provide to a data subject when their data is collected by the controller.

Article 14 [26] is very similar to article 13 but relates to data that was not provided to the controller by the data subjects.

The requirements are broadly similar to Article 13 with an additional requirement to inform the data subject of the source of their data.

There is considerable overlap between articles 13 and 14 in relation the information that must be provided. These requirements has been merged to identify a single set of requirements.

To establish GDPR compliance - based on a Privacy Policy - the presence of the following items will be checked.

- Is the information clear and intelligible?
- Is the information easily accessible?
- Has the controller been identified?
- Does the policy contain the Controller's contact details?
- Is the data (or categories of data) collected identified?
- Are the Purposes of the processing identified?
- Is the Legal Basis for the processing identified?
- Where the Legal Basis is Legitimate Interests, have those interests been identified?
- Where is the data processed?
- Have any recipients of the data been identified?
- Is the Retention Period in the policy?
- Does the policy inform the Data Subject of their rights?
    - Access to data
    - Rectification or erasure
    - Withdrawal of consent (where granted)
    - Objection to processing
    - Data portability
    - Lodgement of a complaint with a Supervisory Authority.

6.6.2 Scoring Compliance

Each criterion listed above will be scored as follows:

Table 1: Compliance Scoring

Result	**Score**
Misleading	-1
Not compliant	0
Partially compliant	1
Compliant	2

The absence of a criterion may lead to that criterion being scored as Not compliant. It was felt that content that was intentionally not compliant or inaccurate to the point of being misleading should not be scored equally with an absence of a criterion. Accordingly, such misleading content will be penalised rather than simply scored as Not compliant. Where a criterion does not apply, it will be scored as Compliant.

7 Analysis and Conclusions

7.1 Analysis of App-Related Data

In addition to the data items collected by the Quest hardware, some ancillary information was gathered in relation to each App to give a more informed picture of the type of Apps that are in the Meta Quest App Store.

App Categories

Apps identify as one category. The sample contains three categories : Games, Apps and Entertainment. By a large margin, most of the Apps in the sample identify as "Games" (75.4%) with "Apps" and "Entertainment" following up with 16.9% and 7.7% respectively.

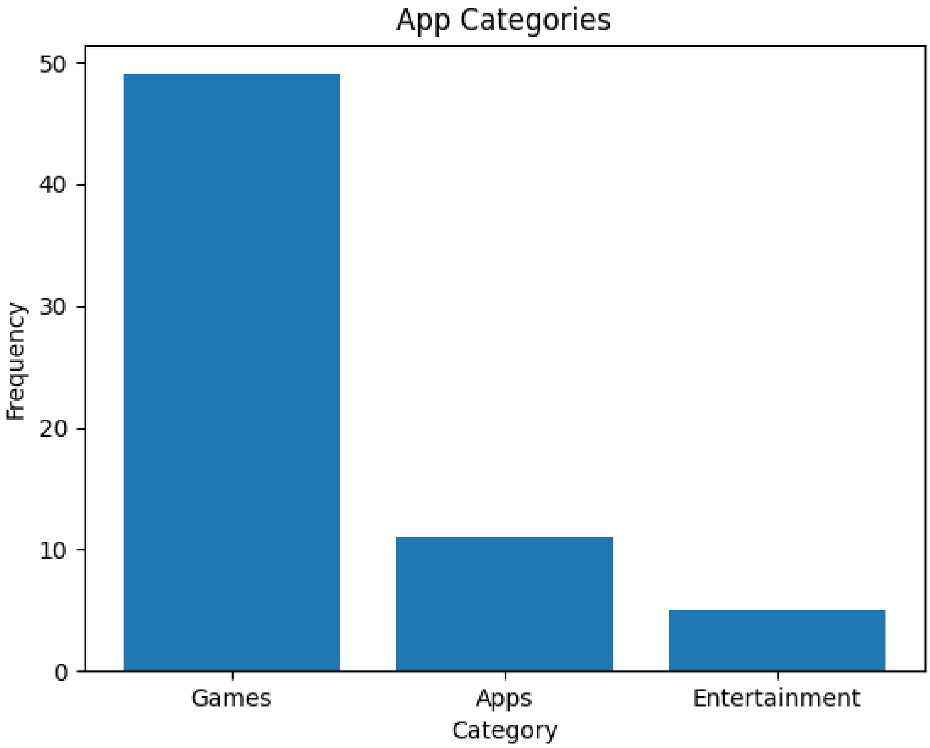


Figure 2: Categories of App

App Genres

Each App can associate with more than one Genre. Almost 85% of Apps associate with either 2 (49.2%) or 3 (35.4%) Genres with 1 and 4 Genres making up the remainder with 7.7% and 4.6% respectively.

22 Apps (33.8%) associate with the "Action" genre and 19 Apps (29.2%) associate with the "Adventure" genre. 7 Apps (10.8%) associate with both genres.

Of the 34 Apps that associate with either or both of the "Action" and "Adventure" genres, all but one identify as Games. The remaining App identifies as Entertainment.

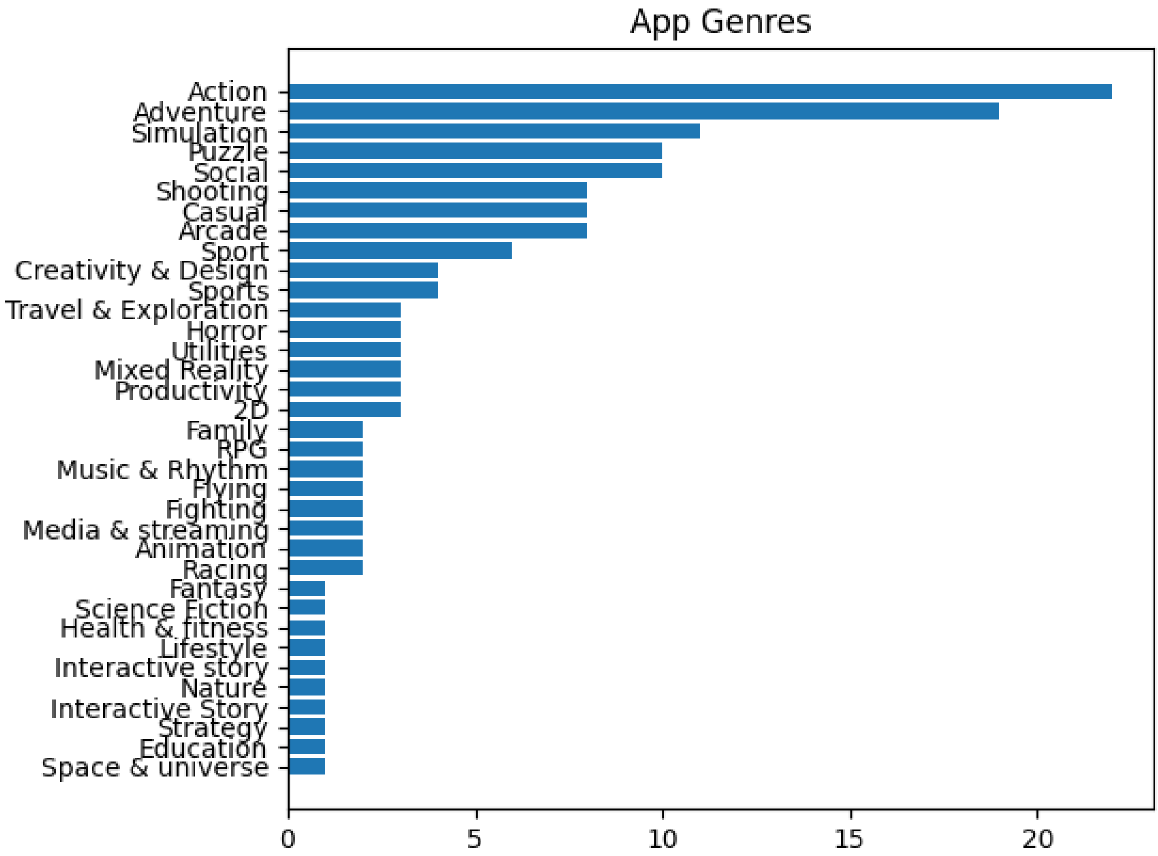


Figure 3: Genres of App

PEGI Ratings

PEGI (Pan-European Game Information) Ratings [27] identify the appropriateness of entertainment content such as games, mobile app, movies or, in this case, Virtual Reality games. They indicate the minimum age that is recommended for the content of the App. It does not rate the difficulty of the game.

Each PEGI rating [28] has an age label and explanation.

Rating	Explanation
3	Suitable for all age groups
7	Contains content that may be frightening to young children
12	May contain bad language of a mild nature, non-realistic violence or sexual innuendo
16	Depiction of violence or sexual activity. Use of alcohol, drugs, smoking or bad language
18	Extreme violence, explicit sexual activity. Suitable for adults only
!	Parental Guidance Recommended

Table 2: PEGI Ratings

Almost half of Apps in the sample (46.2%) are suitable for all ages. A small number (7.7%) have been rated at 18.

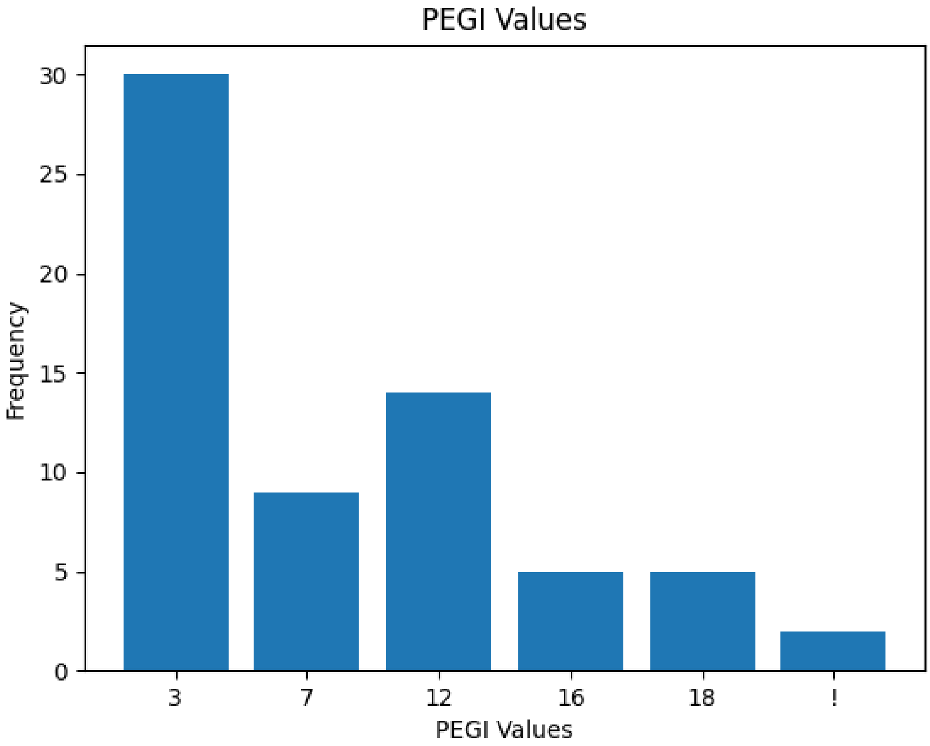


Figure 4: PEGI Ratings

Number of data items Collected

As illustrated in Figure 1 earlier in this report, each app reports the individual data items that it collects. Each app can collect zero to ten data items. This plot depicts the distribution of the number of data items collected by the Apps in the sample.

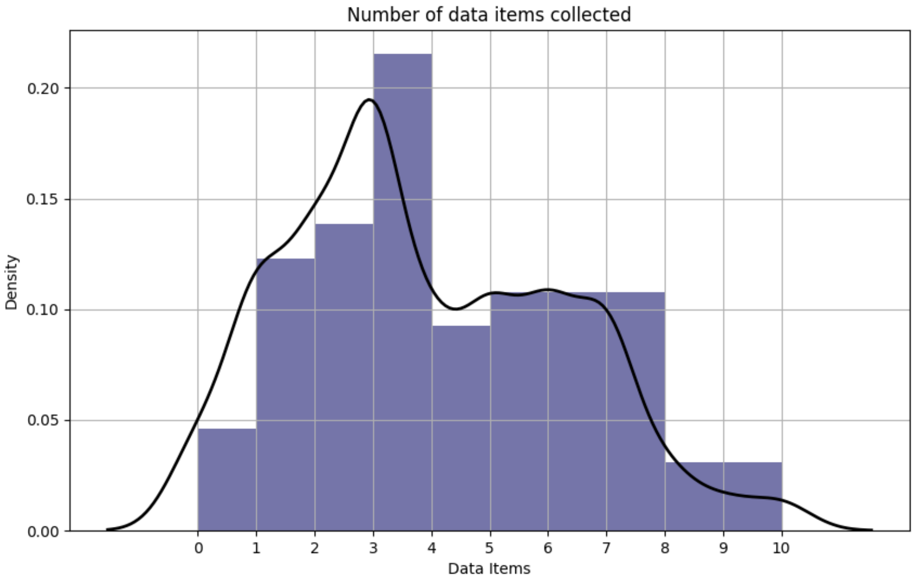


Figure 5: Number of data items collected

It is clear from the plot that that data is skewed somewhat to the right and does not appear to be normally distributed. The specific properties of the data can be established by performing some statistical analysis of the data.

Table 3: Analysis of Data Items Collected

Property	Value
Mean	3.892
Median	3
Mode	3
Standard Deviation	2.373
Skew	0.415
95% Confidence Interval	3.33 to 4.45
Shapiro W	0.955
Shapiro P	0.0193

The Standard Deviation of 2.373 indicates that the dispersion of the data around the mean is moderate. This would suggest that the data is moderately representative.

The positive skew value of 0.415 indicates that there are more values that are significantly higher than the mean than there are significantly below the mean. As the skew value is moderate, the quantity of significantly higher values is not extreme.

The visual judgement that the data is not normally distributed is confirmed by the p-value of 0.0193 from the Shapiro-Wilk test. Because this value is significantly below 0.05 (for 95% confidence), this strongly indicates that the data is not normally distributed.

This is not a flaw or shortcoming in the data. It merely indicates that the data does not follow a normal distribution.

There may be value in obtaining a second (or a larger) sample for performing the same tests and comparing results.

User Data collected

Apps may access multiple User Data items. The UserID and UserProfile are those that are accessed most by apps, at circa 20% for each item.

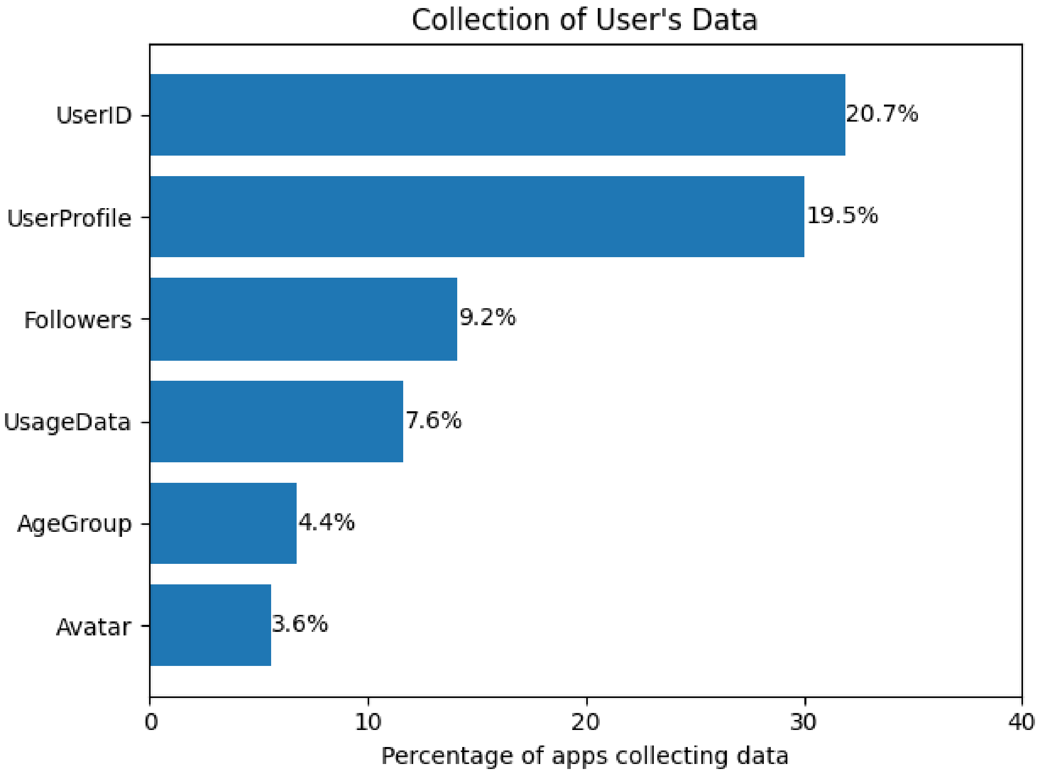


Figure 6: User data collected

Device and Sensor Data collected

Microphone and Storage data are the most accessed Device and Sensor Data. More advanced data, such as Hand and Eye Tracking or Spatial Data are not accessed to the same extent.

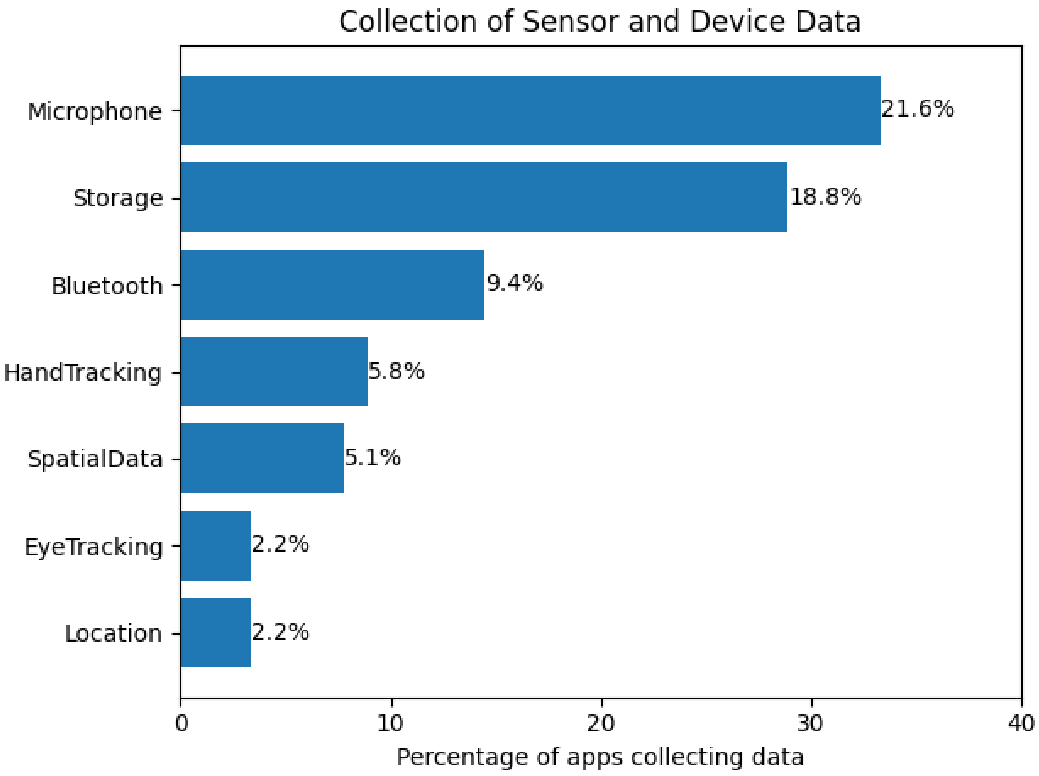


Figure 7: Device and Sensor data collected

7.2 Analysis of Privacy Policies

Compliance

46 of the 65 apps in the sample (70.8%) were found to be generally compliant with GDPR. That is, they were scored at 75% or greater.

Because Apps that do not process data are compliant, it is also helpful to understand the level of compliance among only those Apps that do process data. 12 Apps do not process data. Of the remaining 53 Apps, 34 (64%) are compliant.

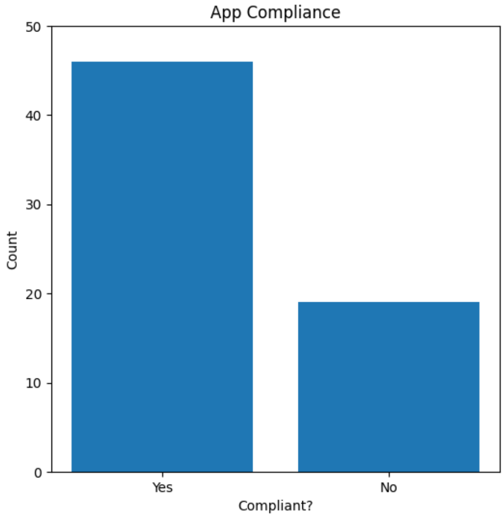


Figure 8: All Apps

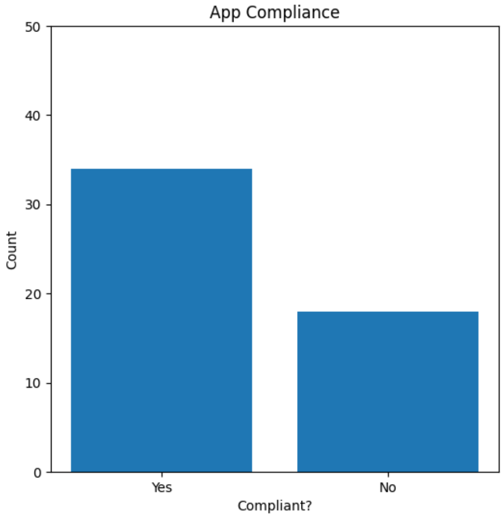


Figure 9: Apps that process data

Compliance Distribution

It is obvious from first glance at the density plot that the compliance levels of the apps do not follow a normal distribution.

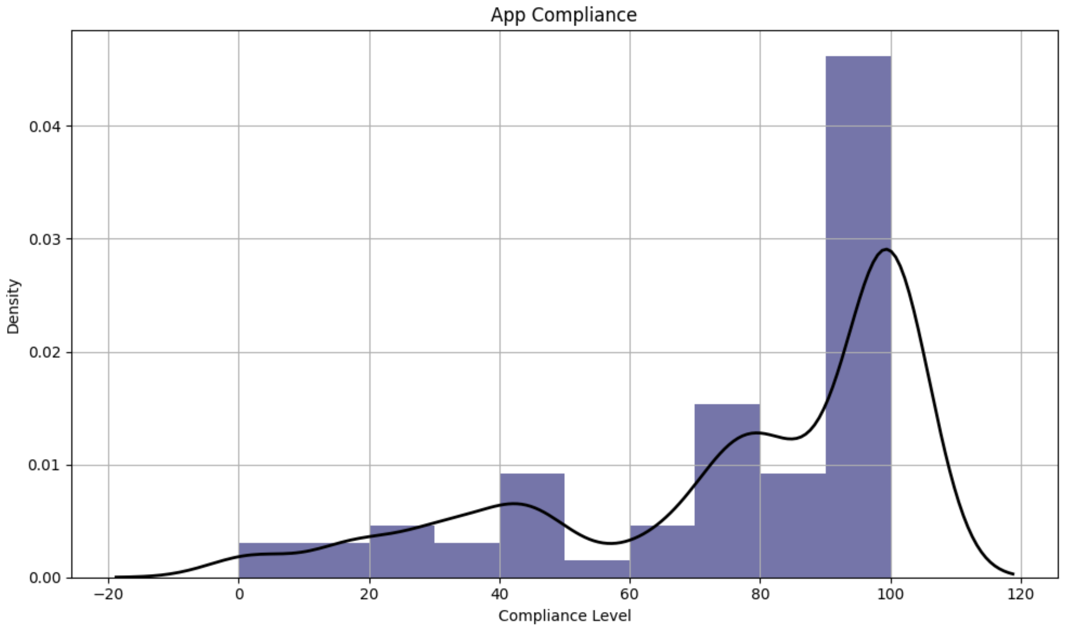


Figure 10: Compliance Density Plot

Table 4: Analysis of Compliance values

Property	Value
Mean	76.282
Median	87.5
Mode	100
Standard Deviation	28.867
Skew	-1.086
95% Confidence Interval	69.26 to 83.30
Shapiro W	0.804
Shapiro P	7.2803 e^{-8}

The Standard Deviation of 28.867 indicates that the dispersion of the data around the mean of 76.282 is relatively significant.

The mode of 100 does confirm the visually obvious clustering of very high values in the plot.

The negative skew value of -1.086 confirms the indications in the plot that the lower side of the plot is longer than the right.

The visual judgement that the data is not normally distributed is confirmed by the extremely small p-value of 7.2803 e^{-8} from the Shapiro-Wilk test. Because this value is extremely small, this very strongly indicates that the data is not normally distributed.

EU Membership

It was observed during the collection of data - and confirmed by the following plot - that those apps where the developer was EU-based appeared to have a greater likelihood of being compliant.

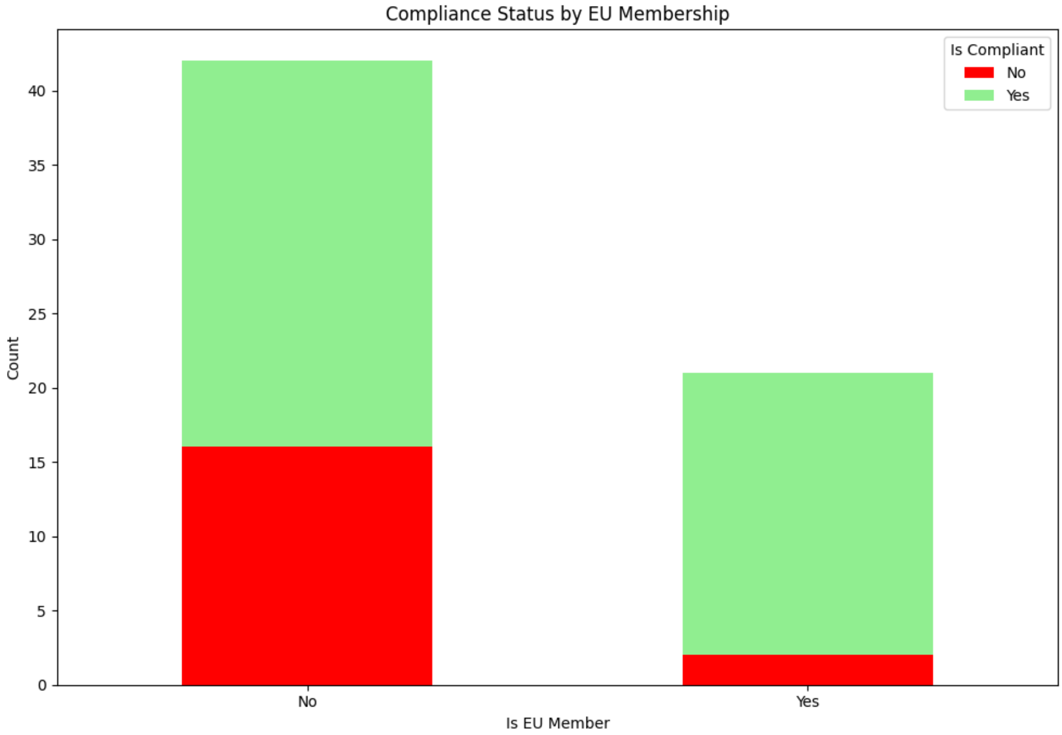


Figure 11: EU Membership and App Compliance

This is not surprising given that GDPR is a European regulation.

There are a number of Data Privacy regulations other than GDPR [29]. It may be that Controllers outside of the EU are more focused on their own regulations and are not as observant of (or perhaps not even aware of) European regulations.

Controller Location

Of those controllers (19) who were identified as not-compliant, almost half (9) were located in North America - USA (6), Canada (3).

This likely reflects the high incidence of USA-based applications. 24 of the 65 apps in the sample (37%) are USA-based.

18 of the 24 USA-based controllers (75%) were scored as compliant which is a higher percentage than the overall compliance level. This indicates that USA-based controllers do not overly contribute to the level of non-compliance encountered.

The remainder of non-compliant apps were located in Japan (4) and one each in France, UK, Brazil, Israel, Sweden and one unknown.

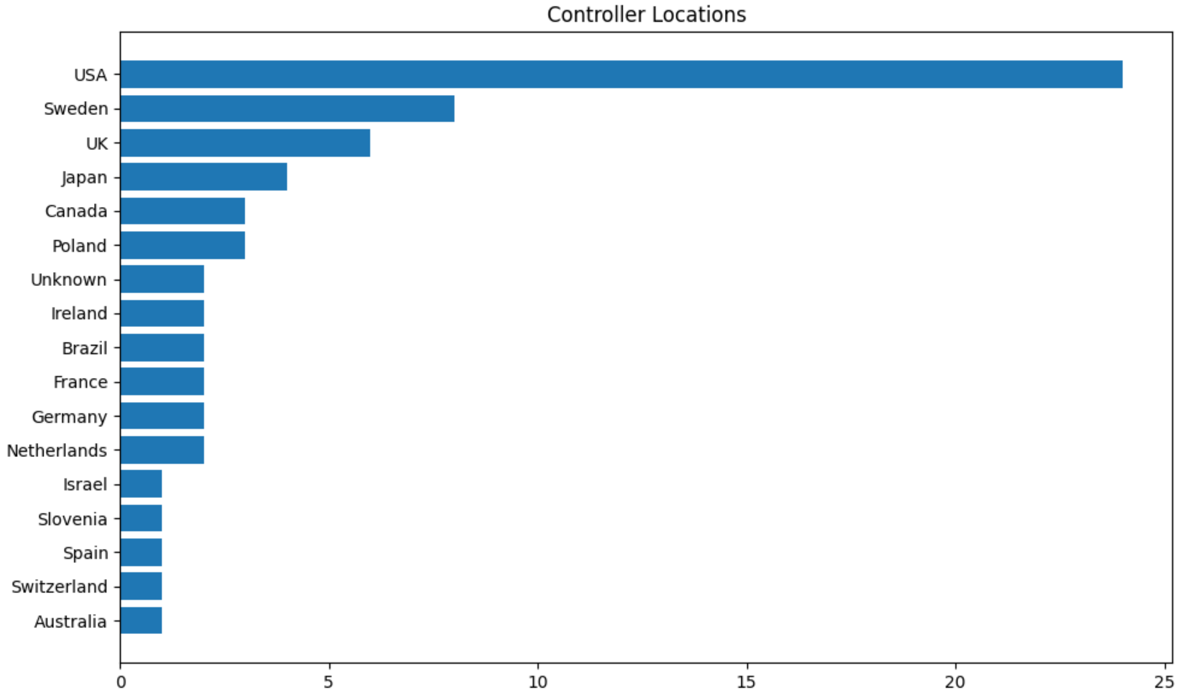


Figure 12: Controller Location

Popularity vs Compliance

The popularity of the sampled apps was estimated by measuring the number of times the app had been rated. Each app was ranked 1 to 65 in order of the number of ratings it had received. The rating value itself was not considered.

No relationship between an app's popularity and its compliance was observed. Indeed, the greatest level of compliance was observed in the middle of the popularity range.

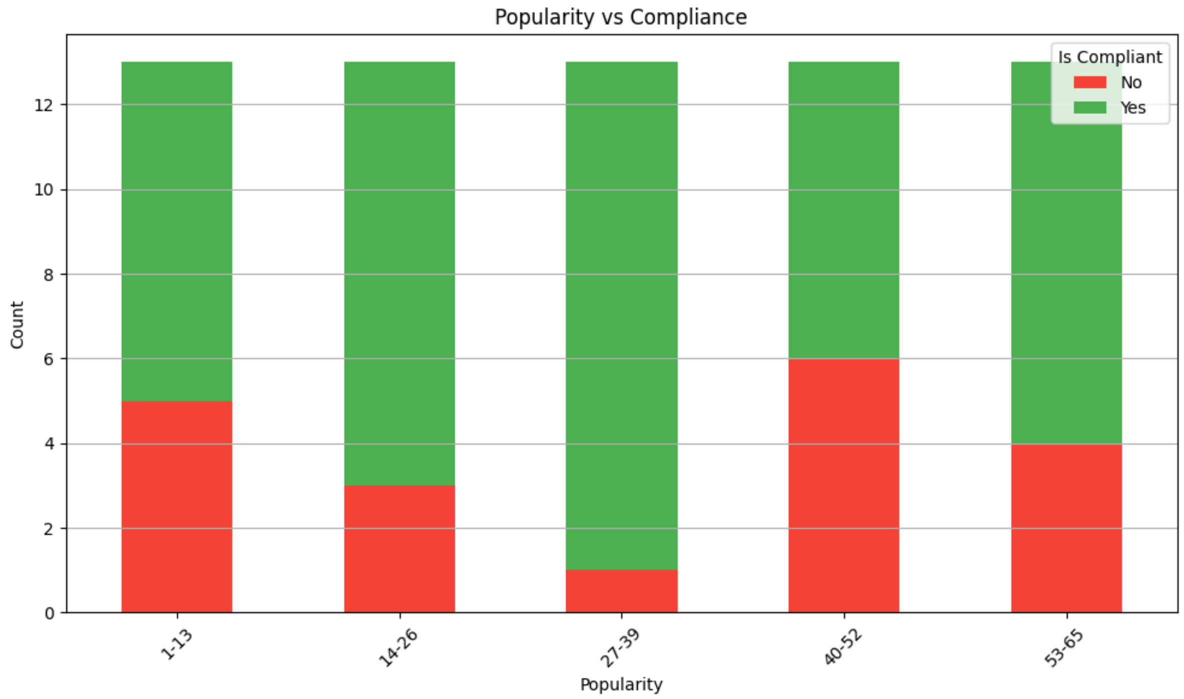


Figure 13: Popularity vs Compliance

7.3 Conclusion

The research question posed in the introduction is ”How compliant with GDPR are applications in the Metaverse?”

Answer: 71% of all assessed Apps were found to be compliant. 64% of Apps that do process data were compliant.

This research does depend on the quality of information provided by the App developers. Given the less than optimal quality of some Privacy Polices, this research may not hold the same value as was anticipated at the outset.

However, the observations in relation to the Privacy Policies may be of interest to the controllers and, perhaps, regulators.

Parents and guardians should, perhaps, exercise diligence in evaluating any Apps that children may be permitted to interact with.

Observations

To answer the research question, a random sample of apps were identified and assessed. The measurement of compliance for each app was based on an interrogation of each App's Privacy Policy.

This approach was somewhat limited in that it represents only a small portion of a controller's GDPR responsibilities. On the other hand, the privacy policy is the most visible expression of the controller's approach to GDPR so it may not be unreasonable to consider it representative of the controller's general approach to GDPR obligations.

There was a certain level of subjectivity in the scoring of many apps. For example, the scoring of the transparency and accessibility of the Privacy Policy was based on this researcher's opinion. On occasion, Performance of Contract or Legitimate Interests may be quoted in the purposes section but were not identified as Legal Bases. The degree to which this is compliant was an opinion which might also be influenced by the quality of the rest of the Privacy Policy.

As the research progressed, it became clear that some developers were unaware of, or did not properly address, their GDPR obligations. There are many Data Privacy regulations worldwide [29] and developers may be focused more on their local regulations to the exclusion of GDPR requirements. Indeed, Canbay et al [12] do raise the issue of incompatibility between different Data Privacy laws. Where a vendor has a worldwide audience, compliance with many different, possibly incompatible, Data Privacy laws may present difficulties.

In other cases, because of a lack of information in the Privacy Policy, it was not clear that the developer did or did not process Personal Data in the App and the Privacy Policy addressed only website-based data collection. There were, additionally, opportunities for the developer to collect Personal Data relating to the app via the creation of an account on the website.

Some Privacy Policies were very clear that they did not gather or process Personal Data from the App. All App developers have the same opportunity to inform the reader of their use (or otherwise) of Personal Data and, indeed, are required by Meta to provide a Privacy Policy.

Accordingly, it has been assumed that an App does process Personal Data unless a Privacy Policy clearly stated otherwise.

An interesting observation was made during the interrogation of Privacy Policies. GDPR Article 12 [24] and Recital 60 of The GDPR advise that "The information .... may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing." The wording is important in that the use of standardised icons is a suggestion, as opposed to a requirement. However, it has been this researcher's experience that the use of standardised icons is the norm rather than the exception - at least for EU-based controllers. Of the 65 Privacy Policies examined, only the Facebook app Privacy Policy contained standardised icons.

7.4 Future Work

An interesting overlap with two papers has been identified.

1. Kharvi proposes [16] a ”Trust Framework for the Metaverse Space” that establishes a Trust Factor score for applications prior to on-boarding.
2. In their ”Study on Oculus Virtual Reality Applications” [17], Guo et al have developed a set of tools for
    a) decompiling and analysing the source code of an App and
    b) assessing the privacy policy of an App

Having observed that privacy policies may exist across multiple files and may make best efforts to meet data privacy requirements while not strictly meeting GDPR requirements, the privacy policy assessment by Guo et al may not fully capture all data privacy elements in a privacy policy.

The authors' tool for code analysis and comparison against the privacy policy helpfully identifies inconsistencies.

A format for privacy policies could possibly be developed with the intent that it would be assessed by a tool for compliance. The policy format - perhaps in JSON format, with mandated headings and content - could improve the accuracy of an automated assessment. Such a format could possibly support multiple data privacy frameworks.

It would be an interesting exercise to attempt to develop such a format that could be used by a refinement of Guo et al's tools to develop a Trust Score as per Kharvi's proposal.

This would require the cooperation of the Meta platform by mandating the use of the new privacy policy format.

8 Appendix

8.1 Meta Data Collection

The "Supplemental Meta Platforms Technologies Privacy Policy" [30] was examined as part of the research for this report to understand what data Meta processes.

Although not strictly within scope of this report, this information was deemed sufficiently relevant to warrant inclusion.

Under the heading "*What information do we collect for Meta accounts?*", the following information is listed:

- Name
- Contact information
- Password
- Date of birth

This data is perfectly reasonable to accommodate account creation.

Under the heading "*What information do we collect for Meta VR Products?*", the list of information is little longer.

Meta Horizon profile

- Profile name
- Profile picture
- Username
- Avatar
- List of followers
- Interactions with games and apps

Physical characteristics and movements

- Position and orientation of your headset and controllers
- Position of your headset, the speed of your controller movement and changes in your orientation
- Your audio data
- Hand and body tracking
- Eye tracking
- Natural facial expressions

The collection of data in relation to characteristics and movements is somewhat of a departure as this information could possibly be classified as biometric in nature.

Indeed, Meta have created a number of separate Privacy Notices to address the new categories of data collected:

- Hand and Body Privacy Notice [31]
- Eye Tracking Privacy Notice[32]
- Natural Facial Expressions Privacy Notice [33]
- Fit Adjustment Privacy Notice [34]

Hand and body sizes are estimated to fit into a generic model which is then used for any app functions. That is, the raw hand and body data is not directly used other than to select an existing generic model and the raw data is then discarded. Hand and body tracking can be disabled on the device. This data can be shared with Apps.

Eye tracking is carried out on the Quest device to create an estimate of where the user is looking. This "abstracted" data is used by the device or Meta servers. The raw eye tracking data is deleted when the abstraction has been created. Eye tracking can be enabled or disabled on the device or for specific Apps. This data can be shared with Apps.

Facial expressions are processed in much the same way as eye tracking. That is, data is processed on the device to identify the facial expression - eg, a smile or a frown. This abstraction - eg smile or frown - is then used to animate the user's avatar. The raw data captured by the device to is not processed beyond its use to identify the expression. Facial expressions data capture can be enabled or disabled on the device or per App.This data can be shared with Apps.

Fit Adjustment is a process whereby the device gathers information about the location of the user's eyes and face in order to assist with an optimal fit. This data is processed only on the device and is deleted after use. It is not shared with any App.

The App developer is required by Meta to process data in line with the various App developers policies, including the Developer Data Use Policy [20]. However, once the data has been shared with an App, Meta has not further control over it. Accordingly, the user should only share data with trusted Apps.

8.1.1 Conclusion

Meta's processing of the data collected on the Quest headset and controllers does appear to be responsible. They are being very transparent about the data collected, the purposes for its collection and how it is used. The use of generic models and abstractions to avoid the direct use of personal data is a demonstration of responsible data use.

Meta's approach does tend to engender trust. However, the responsible approach by Meta should not be assumed to be inherited by Apps on the device and users should not share sensitive with an App unless it is trusted.

8.2 Apps Selected for Assessment

Table 5: Apps selected for assessment

Index	Title
01	Vampire: The Masquerade - Justice
02	Lost Recipes
03	Smash Drums
04	Sniper Elite VR
05	Red Matter 2
06	Racket: Nx
07	Vox Machinae
08	Swords of Gargantua
09	Coursera
10	Time Stall
11	MarineVerse Cup
12	The Light Brigade
13	Blueplanet VR Explore v2
14	Paradiddle
15	Gesture VR
16	Beat Arena
17	Jurassic World Aftermath Collection
18	Star Trek: Bridge Crew
19	YUKI Space Ranger
20	Racket Fury: Table Tennis VR
21	Silhouette
22	Luna
23	Ghostbusters: Rise of the Ghost Lord
24	Death Horizon: Reloaded
25	Cosmonious High
26	Space Salvage
27	Tilt Brush
28	Kill It With Fire VR
29	Little Witch Academia: VR Broom Racing
30	Arashi: Castles of Sin - Final Cut
31	Cybrix
32	Acron: Attack of the Squirrels!
33	Killer Frequency
34	Shores of Loci
35	EverSlaught Invasion
36	Vader Immortal: Episode II
37	Litesport
38	DeoVR Video Streaming
39	Peaky Blinders: The King's Ransom
40	Racket Club
41	Wolves in the Walls

42	Contractors
43	Facebook (Beta)
44	Survivorman VR: The Descent
45	Sweet Surrender
46	The Climb
47	Ghost Giant
48	Job Simulator
49	Unbinary
50	Half + Half
51	WhatsApp for Meta Quest
52	Disc Ninja
53	Eternal Starlight
54	Zoe
55	Carly and the Reaperman
56	The Wizards
57	Homestar VR: Special Edition
58	Henry
59	Wraith: The Oblivion - Afterlife
60	Please, Don't Touch Anything: House Broken
61	Monkey Doo
62	2MD: VR Football Unleashed ALL STAR
63	NFL PRO ERA II
64	Colossal Cave
65	Hellsweeper VR

8.3 Data Collected by Apps

Table 6: Data items collected by Apps

Index	Device and Sensor Data							Your Information						
	Mi	St	Lo	Bl	Sp	Ha	Ey	UID	UP	Av	Fo	UD	AG	Qty
01				Y				Y	Y					3
02														0
03	Y			Y	Y			Y	Y	Y	Y	Y		8
04				Y				Y	Y					3
05							Y	Y	Y					3
06	Y	Y						Y	Y		Y	Y	Y	7
07	Y	Y		Y				Y	Y					5
08	Y							Y	Y					3
09						Y								1
10								Y	Y					2
11	Y	Y		Y				Y	Y	Y	Y	Y		8
12							Y	Y	Y		Y	Y		5
13		Y												1
14	Y	Y						Y	Y	Y	Y			6
15	Y							Y	Y					3
16								Y	Y					2
17								Y	Y					2
18	Y	Y						Y	Y				Y	5
19		Y						Y	Y		Y			4
20	Y							Y	Y		Y			4
21						Y								1
22														0
23	Y	Y			Y			Y	Y			Y		6
24	Y	Y		Y	Y			Y	Y			Y		7
25	Y							Y	Y				Y	4
26								Y	Y					2
27		Y												1
28								Y	Y					2
29		Y						Y						2
30								Y	Y					2
31	Y				Y			Y	Y		Y	Y		6
32								Y					Y	2
33														0
34		Y						Y	Y					3
35	Y													1
36		Y												1
37	Y					Y		Y	Y	Y	Y	Y		7
38	Y	Y	Y	Y		Y		Y				Y		7
39		Y						Y	Y					3

40	Y							Y	Y	Y	Y	Y		6
41		Y						Y	Y					3
42	Y	Y		Y				Y	Y		Y	Y		7
43						Y		Y	Y	Y	Y	Y	Y	7
44								Y	Y		Y			3
45		Y	Y	Y				Y	Y		Y			6
46								Y	Y		Y			3
47	Y	Y												2
48						Y		Y	Y				Y	4
49		Y												1
50	Y							Y	Y		Y	Y		5
51	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y	10
52	Y							Y	Y		Y	Y	Y	6
53	Y			Y		Y		Y	Y					5
54	Y	Y			Y			Y	Y	Y	Y	Y	Y	9
55	Y							Y	Y					3
56		Y						Y	Y					3
57	Y													1
58		Y						Y	Y	Y	Y	Y	Y	7
59		Y						Y	Y					3
60					Y	Y		Y	Y					4
61	Y							Y	Y			Y		4
62		Y		Y				Y	Y		Y			5
63	Y							Y	Y		Y	Y	Y	6
64	Y				Y		Y							3
65	Y			Y				Y	Y		Y			5

Table 7: Key

Key	**Data**
Mi	Microphone
St	Storage
Lo	Location
Bl	Bluetooth
Sp	Spatial Data
Ha	Hand Tracking
Ey	Eye Tracking
UID	User ID
UP	User Profile
Av	Avatar
Fo	Followers
UD	Usage Data
AG	Age Group
Qty	Quantity of data items collected

8.4 Privacy Policy Analysis

Table 8: Privacy Policy Analysis

Index	Data	Cl	Ac	Id	Co	Da	Pu	Le	Li	Pr	Rec	Ret	Ri	Total	Compliance
01	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
02	No														100%
03	Yes	1	1	2	1	1	1	1	1	1	1	1	1	13	54.2%
04	Yes	1	2	2	2	2	2	1	1	1	2	2	1	19	79.2%
05	No														100%
06	Yes	1	1	1	1	1	1	0	0	0	1	0	0	7	29.2%
07	Yes	0	0	1	1	1	1	0	0	0	0	0	0	4	16.7%
08	Yes	-1	1	2	2	1	2	0	0	2	1	0	1	11	45.8%
09	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
10	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
11	Yes	1	2	2	2	2	2	2	2	0	2	2	1	20	83.3%
12	Yes	0	0	1	1	0	0	0	0	0	2	0	1	5	20.8%
13	Yes	0	0	0	0	1	0	0	0	0	0	0	0	1	4.2%
14	Yes	0	0	2	2	0	0	0	0	2	2	0	0	8	33.3%
15	Yes	0	0	1	1	1	0	0	0	0	1	0	0	4	16.7%
16	Yes	0	1	2	1	1	2	0	0	0	1	2	0	10	41.7%
17	No														100%
18	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
19	Yes	0	1	1	1	1	2	0	0	2	0	0	0	8	33.3%
20	Yes	2	2	2	2	2	2	2	2	0	1	2	2	21	87.5%
21	Yes	1	2	2	2	2	2	0	0	1	2	2	2	18	75%
22	Yes	1	1	2	2	2	1	0	0	0	2	0	0	11	45.8%
23	Yes	2	2	2	2	2	2	0	0	2	2	2	1	19	79.2%
24	Yes	1	1	2	2	0	1	0	0	0	0	0	0	7	29.2%
25	Yes	1	1	2	2	1	1	2	2	1	2	2	1	18	75%

26	Yes	2	2	2	2	2	2	2	2	0	2	2	2	22	91.7%
27	Yes	1	1	2	2	1	1	2	2	1	2	2	1	18	75%
28	Yes	2	2	3	3	2	2	1	1	2	2	2	2	24	100%
29	Yes	1	1	2	1	2	2	0	0	0	1	0	1	11	45.8%
30	No														100%
31	Yes	2	2	2	2	2	2	0	0	1	2	2	1	18	75%
32	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
33	Yes	2	2	2	2	2	2	2	2	1	2	2	2	23	95.8%
34	Yes	1	1	2	1	1	2	1	1	0	2	2	1	15	62.5%
35	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
36	Yes	1	1	2	2	2	2	0	0	1	2	2	1	16	66.7%
37	Yes	2	2	2	2	2	2	1	0	2	2	2	2	21	87.5%
38	Yes	2	2	1	1	2	2	2	2	2	2	1	2	21	87.5%
39	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
40	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
41	Yes	1	2	2	1	2	2	2	0	2	2	2	2	20	83.3%
42	Yes	1	2	1	1	1	0	1	0	0	0	2	1	10	41.7%
43	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
44	Yes	1	2	2	2	2	2	0	0	0	2	2	1	16	66.7%
45	No														100%
46	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
47	Yes	0	0	0	0	0	0	0	0	0	0	0	0	0	0%
48	Yes	1	1	2	2	1	1	2	2	1	2	2	1	18	75%
49	No														100%
50	Yes	1	1	1	1	1	2	2	2	2	2	2	2	19	79.2%
51	Yes	2	1	2	2	2	2	2	2	2	2	2	2	23	95.8%
52	No														100%
53	No														100%
54	Yes	2	2	2	2	2	2	0	0	2	2	2	2	20	83.3%

55	Yes	1	2	2	2	2	2	0	0	1	2	2	2	18	75%
56	No													0	100%
57	Yes	1	1	1	1	2	2	0	0	0	2	0	0	10	41.7%
58	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
59	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
60	No														100%
61	Yes	1	2	2	2	2	2	1	0	2	2	2	1	19	79.2%
62	No													0	100%
63	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%
64	No														100%
65	Yes	2	2	2	2	2	2	2	2	2	2	2	2	24	100%

Table 9: Key

Key	**Data**
Data	Is personal data processed?
Cl	Is the information clear and intelligible?
Ac	Is the information easily accessible?
Id	Has the controller been identified?
Co	Does the policy contain the controller's contact details?
Da	Have the data (or categories of data) been identified?
Pu	Have the purposes of the data processing been identified?
Le	Have the Legas Basis or Bases been identified?
Li	Where the Legal Basis is Legitimate Interests, have those interest been identified?
Pr	Has the location of the processing of the data been identified?
Rec	Have recipients of the data been identified?
Ret	Has the retention period (or means for calculating it) been identified?
Ri	Does the policy identify the Data Subject's rights?
Total	Score Total
Compliance	Level of compliance

8.5 Privacy Policy Observations

Table 10: Privacy Policy Observations

Index	Title	Observations
01	Vampire: The Masquerade - Justice	https://www.fasttravelgames.com/privacy-policy? This policy does not include the right to make a complaint to a Supervisory Authority. Otherwise, this is an excellent policy.
02	Lost Recipes	https://www.schellgames.com/lost-recipes-privacy-policy? The app does not report (in its play store entry) that it collects any data. The Privacy Policy states that it only collects anonymised data and that it “does not collect the player’s name, physical address, contact information, or any geolocation information.” It also states that “We aggregate all information collected so that it cannot be used to identify any particular player.” Aggregated and anonymised data is not Personal Data. Accordingly, this application is entirely compliant with GDPR.

03	Smash Drums	https://privacy.smashdrums.com/? The game is developed using tools from Unity Analytics – a game insights and analytics company. The app developer is, however, still responsible for the data processed by this third party. The app refers users to a third party's (Unity) privacy policy. The user is further referred onwards to another privacy policy for apps. Unity's privacy policy is quite generic, and it is not clear what information they collect within this app. The controller appears to have abdicated their responsibility to a third party's generic privacy policy. The information is, therefore, unclear, not easy to access and does not use standardised icons. The identity and contact details of the controller consists of its name and an email address. No physical address or phone number is included. The email address, contact@smashdrums.com, is a generic email address, not a privacy-related address. The contact details have been judged to be partially compliant. There is inconsistency between the data collection that is reported in the App Store's entry and the privacy policies. Although Unity's privacy policy is quite comprehensive, it is difficult to understand to what extent any particular section of it applies (if at all) to this current app. Accordingly, any scoring relating to its contents have been scored at a maximum of "Partially Compliant".
04	Sniper Elite VR	https://rebellion.com/privacy? Although this app's Privacy Policy does make efforts to be clear, there is no Legal Basis header. Legitimate Interest is referred to as the legal basis for processing data, but this is buried in the Third Parties section. It defines personal data as "data about you from which you could be identified – such as your name, your date of birth, your contact details" which is not an accurate definition. This resembles a definition of PII (Personally Identifiable Information) which is an American data privacy concept. Although most rights are present, they are not accompanied with standardised icons and no reference to making a complaint to a Supervisory Authority is included. Otherwise, it scores well.
05	Red Matter 2	http://verticalrobot.com/privacy/? The app developer's privacy policy is very succinct. They do not collect, store or process user data. Any data processing is carried out on the local device.

06	Racket: Nx	https://racketnx-public.s3.us-west-1.amazonaws.com/racket-nx-privacy.html? The policy is old (2017) short, poor and entirely inadequate. The wording in the policy indicates that this was written to (poorly) comply with data protection regulations other than GDPR. The developer's name is included but no physical address or, phone number. Two different email addresses are supplied – one for data deletion and one for general privacy enquiries. The data that is being collected is not fully identified nor are the purposes for the processing. There is no rights section, no legal basis, no standardised icons or retention period. This is a very poor policy.
07	Vox Machinae	http://voxmachinae.com/privacy.shtml? The (very short) policy refers to two entities - Vox Machinae and Space Bullet Dynamics Corporation. It is not clear which of these is the controller. There is a single email address (not a privacy email address) provided for contact – no physical address or phone number. The data processed is listed however its purposes are not comprehensive. Accordingly, some uncertainty remains in relation to the accuracy/completeness of the data/purposes claimed in the policy. That is the entirety of the policy.

08	Swords of Gargantua	https://www.thirdverse.io/en/privacy-policy? The policy identifies Japan as the location of processing and includes a clause that deems the user to have agreed to the transfer of their information outside of the EU. The requirement for compliant third country transfers is not consent-based, and this clause is inaccurate and misleading. Additionally, the policy deems that the user agrees to their information being processed, stored or transferred according to the policy. Again, compliance is a legal requirement, not consent-based. It also deems the user to have acknowledged that Japan may not afford the same rights and privacy as local laws. Data collected is reasonably comprehensive but is a generic description of data collected by all apps or websites or forums controlled by the controller. This does not specifically describe data collected by this app and, accordingly, does not allow a user to make an informed decision about the use of the app based on the data being collected. Uder GDPR, the controller is responsible for the security and safety of personal data under its control. This policy advises that it cannot guarantee non-disclose and specifically disclaims warranties in relation to unauthorised disclosure. This is entirely in conflict with their GDPR responsibilities. Retention of data will be implemented in accordance with their document retention policy. However, that policy is not stated, nor is there a link to it. Transfers to third parties are referenced but are unclear and vague. No legal bases are identified. While rights are acknowledged and listed, they are listed in a single sentence with no standardised icons. Given the misleading information provided to the user, this app has been penalised (-1) under the heading of Clear and Accessible.

09	Coursera	https://www.coursera.org/about/privacy? The privacy policy advises that it covers “information we collect from you through our Site”. It does not reference the app specifically. However, given that the app is another method of accessing Coursera’s training data, it may be assumed that the app is covered. The privacy policy appears to have been drawn up to satisfy US regulatory obligations. However, it is clear that the controller has expended considerable efforts to comply with GDPR requirements.
10	Time Stall	https://vertigo-games.com/privacy-policy/? This is a well laid out, comprehensive policy. One minor item was observed – the legal basis of Legitimate Interests is described as a “Processing Ground”. This is not considered sufficient to reduce the score from “Compliant” to “Partially Compliant”.
11	MarineVerse Cup	https://www.marineverse.com/privacy? The policy is quite good generally. However, rights are not in a single block of text and are spread out over different headings. Data portability is not mentioned. The retention period of 7 years does seem excessive. However, the policy is transparent about its period. Legitimate Interests is identified in the policy but not under a heading of legal basis. However, legal basis is mentioned in the same paragraph so, on balance, this has been deemed to be compliant. The policy states that “To the extent permitted by law, we accept no liability for any breach of security, etc, etc”. It does then acknowledge its obligation under GDPR to report breaches to data subjects. However, because of this conflict with their GDPR responsibility and the earlier minor issues, the app has been docked 1 point for transparency & clarity.

12	The Light Brigade	http://funktroniclabs.com/legal? This policy is quite bare. The controller's name and an email address is provided. The email address is a standard support email address. No physical address or phone number is provided. It is unclear to what activities the policy refers as there is no information that appears to relate to the app. The data collected is not identified and the purposes are vague and insufficient. Rights are included in a single sentence and are incomplete.
13	Blueplanet VR Explore v2	https://blueplanetvr.com/wp-content/uploads/2022/11/BPVR_PRIVACY.jpg? The privacy policy is an image of some text that advises that they do not collect "identifiable personal information" but that they do collect "analytical information about our distribution". Without a definition of "identifiable personal information" and a list of information that they gather that does not meet that definition, it is not possible to understand what data is actually collected. They do advise that they collect data from their website such as IP address, browser type and version, pages visited and date/time and duration of visit. This is personal information but there is no further information on what they do with this, its retention period, purposes, etc. Accordingly, this policy scores only a single point for being partially compliant in identifying the data it processes.
14	Paradiddle	http://paradiddleapp.com/privacy-policy? This policy appears to be entirely based on US/California law and appears to refer to its website and not the app. The data collected is not identified and its purposes appear website related. There is no retention period, nor legal basis identified. The right to have data deleted is included. However, this is insufficient on its own to be compliant.

15	Gesture VR	https://www.gesture-vr.com/privacy-policy? The controller's name and an email address are provided. The email address (hello@gesture-vr.com) is a standard contact email address. No physical address or phone number is provided. Some data is identified as being collected directly but this appears to be related to the website and contact made by users. The policy states that "Gesture VR does not collect any stats or analytics that contain personal information". However, it is unclear if it does collect data that it does not consider to be personal data. Additionally, as this is a Canadian company, its definition of personal data may differ to that of the EU. It identifies third parties that it uses that may collect data, but it does not identify the data nor its purposes. No legal basis has been identified and rights are simply not mentioned at all.
16	Beat Arena	https://legal.konami.com/games/privacy/? Although the controller's identity is provided (as is a physical address), no email address or phone number is provided. As the company is based in Japan, a phone number of email address is required for reasonable contact. A form exists that can be used to request access to data or to have data deleted or consent withdrawn however this requires navigating through two separate pages to reach it. Additionally, the user is advised that a fee may be chargeable for this access. This is not considered compliant. Some information collected is identified but it is unclear if this relates to website usage, app usage or other. Purposes are provided but these are accessible on a different page. Disclosure to third parties is unclear. The policy refers to California Privacy Rights but not to The GDPR.

17	Jurassic World Aftermath Collection	https://coatsink.com/privacy-policy? At the top of this privacy policy is a link that users can click to “complete a GDPR Data Request”. Upon clicking the link, the user is brought to a page that appears to refer to a GDPR form but that does not display it. On this broken page, there is a link to the “official EU GDPR website” which is eugdpr.org. This is not the “official EU GDPR website”. Indeed, clicking on the link redirects the user to an insecure web page (ie no https) advertising a skin product. The identity and contact details are very clear and comprehensive. Although this policy got off to a poor start, it appears that the app does not collect data about the user. That is the device information and country is provided by the platform in an aggregated manner, but the user is not identified. Other data is collected and processed. However, this is unrelated to the app and is out of scope. Accordingly, no personal data is being processed and the app is entirely compliant.
18	Star Trek: Bridge Crew	https://legal.ubi.com/privacypolicy/? This is a very comprehensive Privacy Policy. It does start off unfortunately by mis-defining personal data. It also does not use standardised icons for rights. Otherwise, this policy appears to be compliant in every respect. They have clearly made significant efforts to protect the rights of users and to comply with privacy regulations.

19	YUKI Space Ranger	https://arvore.io/privacy-policy/yuki/? The privacy policy for this game is part of a “Terms of Services and Privacy Policy” document. The name of the controller is at the top of the document and an email address is provided at the bottom. The information in this document – it can’t be called a privacy policy – was difficult to read and was presented more like a contract than a document designed to inform data subjects of their rights. The policy states that it only collects anonymous data from the device. This includes “. . . . information about the virtual reality headset, interactions with the Software, biofeedback and biometrics information, geographic locations . . . ” This information cannot be gathered anonymously. This is personal data, even if the information does not identify the data subject. Indeed, as biometric data is classified as “Special Category Data”, it requires a raised level of attention for processing. Rights are not mentioned, nor retention policy. Legal basis is, similarly not addressed. It states that “We will never share your personal information with third parties that are not bound by our Privacy Policy unless you tell us otherwise. . . ” This is very unclear. It is not known if they do or do not shared information with third parties. They do not mention other parties.
20	Racket Fury: Table Tennis VR	https://www.pixeledgegames.com/privacy-policy-games? This is a good privacy policy. It starts out strongly by identifying the user’s rights – although it does name the UK Data Commissioner as the contact for any complaints. It would appear that this policy is aimed at UK readers. The specific piece of data that are processed are identified as It does make a small error in that it states that its legal bases are performance of contract or legitimate interests but that users can withdraw consent. This is not accurate. However, it is a very minor oversight. They don’t identify where the data is processed and are vague about third parties. Otherwise, this is quite a good privacy policy.

21	Silhouette	https://beyondframes.com/privacy-policy? Rights are listed in a detailed and comprehensive manner – although not with standardised icons. The policy states that "we may share information about you with certain third parties based on the legal basis in Articles 6(1)(b), 6(1)(c) and 6(1)(f) of the GDPR as follows:". However, it does not actually identify any legal basis for the processing. Although it doesn't state that processing is carried out in the EU, the controller will transfer the data based on privacy shield or standard clauses. However, privacy shield was struck down in 2020 by the ECJ. This is a significant legal inaccuracy, and the Transparency score has been docked 1 point.
22	Luna	http://www.funomena.com/privacy? Although the controller comprehensively identifies data that is collected, its purpose is very vague. The only right mentioned is deletion. However, this is not compliant : "We will use commercially reasonable efforts to honor your request. We may retain an archived copy of your records as required by law or for legitimate business purposes." The policy relies on "Safe Harbour" for third country transfers. This was struck down in 2015 prior to the introduction and subsequent striking down of "Privacy Shield". Given that the date of the policy is 2021, this is an inexcusable legal error. There is no legal basis or retention period and no processing location.
23	Ghostbusters: Rise of the Ghost Lord	https://www.sonypictures.com/corp/privacy.html? Although this is a very comprehensive policy, it was developed for US data subjects and does not address GDPR requirement. By virtue of its comprehensive approach, it does satisfy a number of the test applied. However, it contains no legal basis and only partially satisfies the rights test.

24	Death Horizon: Reloaded	http://deathhorizon.com/privacy-policy/? This developer claims not to collect or process personal data. However, it identifies specific third parties that it uses to provide services, which may collect and process data. This is entirely insufficient. As the controller, the developer is responsible for the data collected and processed by third parties on its behalf. It is not sufficient to simply refer the reader to these third parties. The App Store information on the app indicates that it processes the following data: Microphone, storage, Bluetooth, spatial data, User ID, user Profile, Usage data. It is not unreasonable to speculate that some of this may be processed by the third parties. The lack of information in this policy combined with the abdication of its responsibilities has resulted in this game scoring very poorly.
25	Cosmonious High	https://owlchemylabs.com/privacy? According to its “About Us” page, Owlchemy Labs was acquired by Google in 2017. Click on the Privacy Policy link takes the user to Google’s very extensive Privacy Policy pages. Although the policy is very comprehensive, it covers all services offered by Google and does not address the data nor purposes or other GDPR requirements that are specific to the app. For these reasons, although the policy scores highly for the inclusion of information required by GDPR, its relevance to the app is unknown and the policy has been deemed partially compliant for clarity and accessibility. There is no information on where the processing takes place but there is detailed information on third country transfers. Rights are mentioned all in a single sentence. The policy and controls are very comprehensive, and Google makes available some tools with which users can manage their data. However, as relates to this app, their policy is a little lacking.
26	Space Salvage	https://fruitysystems.com/privacy-policy/? This privacy policy, though shorter than many others, addresses almost all of the requirements in a clear, concise and plain fashion.

27	Tilt Brush	https://www.google.com/intl/en/policies/privacy/? This is a Google-owned app and its score has been copied from the earlier assessment of Google's privacy policy
28	Kill It With Fire VR	https://www.tinybuild.com/privacy-policy? This policy addressed most GDPR requirements. It mentions the controller's legitimate interests under purposes and references consent elsewhere but does not identify these specifically as legal bases. Otherwise, this is a good policy.
29	Little Witch Academia: VR Broom Racing	https://lwa-vr.com/privacy-policy/? This policy is based on Japan's Personal Information Protection Act. GDPR is not addressed at all. While is some overlap between the two regulations, this policy lacks a number of requirements to be compliant with GDPR. There is only a physical address provided for contacting the company in Japan) Legal bases are not identified. Rights are not addressed correctly. No retention period is identified.
30	Arashi: Castles of Sin - Final Cut	https://skydance.com/sdi-privacy-policy/? This app does not process personal data. There was initially some uncertainty about the accuracy of the company's claims (because they are so easy to make). However, the company has an enterprise privacy policy in addition to the game-specific policy. The enterprise privacy policy is very comprehensive. Accordingly, the company's claims to not process personal data is assumed to be accurate and the app is complaint.

31	Cybrix	https://www.holonautic.com/privacy-policy? This is a reasonable policy. It does make an error in that it assumes consent for third country transfers. This is not consent-based. Legal Basis is not identified. It is only mentioned in relation to consent from a parent for processing of a child's information. The only right identified is that of deletion.
32	Acron: Attack of the Squirrels!	https://www.resolutiongames.com/privacy? While this policy does makes efforts to address GDPR, it makes the common US-based mistake in relation to personal data by defining it as "any information that, directly or indirectly, can identify a natural person" which is not how GDPR defines personal data. Otherwise, this is a comprehensive and compliant policy
33	Killer Frequency	https://www.team17.com/privacy-policy/? This policy does make the all-too-common error of referring to Privacy Shield for transfers to the US. Otherwise, this is a comprehensive policy that clearly and transparently identifies the data used, its purposes, legal basis, retention and user rights.
34	Shores of Loci	https://shoresofloci.com/lociprivacypolicy_feb2022/? This policy makes the usual mistake of identifying personal data as that which identifies a user. This is the US definition and is not consistent with GDPR. The policy advises readers that information is used in a particular way "because we have a legitimate interest in doing so". This is not identified as a legal basis. Not all rights are conveyed to the reader.
35	EverSlaught Invasion	https://fasttravelgames.com/privacy-policy? Same as 01 Vampire: The Masquerade - Justice

36	Vader Immortal: Episode II	https://privacy.thewaltdisneycompany.com/? This is a Disney game and policy, and it identifies personal data as described a number of times earlier by US companies. There is no mention of GDPR and this is entirely addressed towards US regulations and users. There is no legal basis and, although some rights overlap with those required by GDPR, they are only partially compliant. The policy is more of a legal document and is spread across a number of pages. It does not read well and not clear using plain language.
37	Litesport	https://litesport.com/privacy? This policy makes efforts to address GDPR concerns. However, its attempt to address legal basis is ineffectual. It simply describes most of the various legal bases (the one absent being public interest). It does not assign a legal basis to any particular form of processing. Nor does it describe the legitimate interests that it may have. This is the only issue with this policy. It attempts to address US, Canada, UK, California and EU regulations. The various regulatory jurisdictions do, doubtless, cause difficulties for controllers attempting to comply. Although rights are all identified in a single sentence, they are all itemised and also includes the right to complain to a SA.
38	DeoVR Video Streaming	https://deovr.com/pages/privacy? It took some sleuthing to establish where DeoVR is based. There was no information in its privacy policy, terms of service, Contact us, About us pages, etc. Otherwise, the policy is generally compliant. The retention period is not advised to the reader, nor the criteria for deciding it. Only that data will be retained as long as legally permitted. This is not what GDPR requires.
39	Peaky Blinders: The King's Ransom	https://www.maze-theory.com/legal/#privacy? This is a good policy which addresses all of GDPR's requirements.

40	Racket Club	https://www.resolutiongames.com/privacy? This is the same controller and same policy as 32: Acron: Attack of the Squirrels! The scores from that app have been copied to this one.
41	Wolves in the Walls	https://fable-studio.squarespace.com/legal/privacy Same issue with the definition of Personal Data and it talks later about "personally identifiable information" – a US concept. Otherwise, the policy starts off well with definitions. It makes significant efforts at compliance but omits the legitimate interests it claims.
42	Contractors	There was no information on the controller other than the name. There was a second name which appears to be related. However, the location or contact details (other than an email address) were not present and were not discovered after a small amount of research. The policy appears to be incomplete. It does not contain any information under the "WHAT INFORMATION DO WE COLLECT?". It also reported that "Our servers are located in. " The only data that it reports as being used is: "We use the information we collect or receive: Video Game User ID" Which is somewhat confusing. It lists legal bases that "may" be used but does not identify any legal bases that it does rely on nor what its legitimate interests are. International transfers and sharing are subject to the same lack of specificity. Not all rights are advised to readers. "You have the rights to review, change, or terminate your account at any time." It also identifies the right to complain.
43	Facebook (Beta)	https://www.facebook.com/privacy/policy/?entry_point¯data_policy_redirect&entry¯0 This is a comprehensive and high scoring policy which addressed all GDPR concerns fully.

44	Survivorman VR: The Descent	https://survivormanvr.com/privacy-policy-1 This was a very difficult policy to read. Dense blocks of legalese goes directly against the spirit and intent of GDPR for clarity and transparency using plain language. It is not clear if the company does or does not process personal data. It advises that it does not but then proceeds to describes its use of such information and its legal basis. Rights are addressed comprehensively but are presented in a very difficult to process manner. Purposes and legal basis appears to have been confused by the company. No legal basis has been identified.
45	Sweet Surrender	https://www.salmi.de/privacy/ It appears that this app does not collect or process personal data.
46	The Climb	https://www.theclimbgame.com/privacy Excellent policy that addresses all GDPR requirements.
47	Ghost Giant	https://thunderfulgames.com/privacy-policy/ This privacy notice advises that "This notice does not relate to information processed when playing our games." There is a specific privacy policy that covers a different game (LEGO® Bricktales) but there is no information relating to, or links to, a privacy policy that covers this game. In the absence of a privacy policy, or information indicating that it does not process data, the app has been scored at zero.
48	Job Simulator	This is an Owlchemy Labs app – now owned by Google. The previous score has been copied.
49	Unbinary	https://unbinary.com/privacy-policy/ The company claims to only process anonymised data from the game. Accordingly, no personal data is processed and this is 100

50	Half + Half	https://nock.game/privacypolicy This policy does not specifically mention the game and refers generically to “services” The identity and contact details for the company are minimal. Otherwise, the policy scores well.
51	WhatsApp for Meta Quest	https://www.whatsapp.com/privacy The URL for the privacy policy for this app links to a page describing how the app secures data as opposed to how the company processes personal data in accordance with appropriate regulations. As this is a Facebook app, it is assumed that the processing is carried out in accordance with Facebook’s privacy policy which has already been assessed in this report. The Facebook score has been copied for this app but it has also been docked a point for accessibility.
52	Disc Ninja	https://immersion.games/game-privacy-policy The policy reports that “The Application does not collect any precise information about the User’s identity, User or device real time location nor any data that can be used to track the User’s activity.” Given that some policies use an incorrect definition of personal data, it is difficult to accept with 100 However, at this point, the claim must be taken at face value unless other evidence exists to invalidate this claim
53	Eternal Starlight	https://www.starlight-vr.com/pages/privacy.html No data collected. “We take privacy seriously and aim to collect as little information as possible. Eternal Starlight Eternal Starlight does not currently collect any information from users and does not store any information on external servers or websites. We do not store any user names, scoreboards or any other information.”

54	Zoe	https://zoeimmersive.com/privacy-policy/ A good policy that meets most of the GDPR requirements with the exception of legal basis which is entirely absent
55	Carly and the Reaperman	https://beyondframes.com/privacy-policy/ Same developer/controller/policy as 21 Silhouette. Scores have been copied down.
56	The Wizards	https://www.thewizardsgame.com/wp-content/Privacy.pdf “It is hereby confirmed that The Wizards (the “Software”) does not collect any User data or personal information. As such no personal information or other User data is being stored, processed or transferred by Carbon Studio Sp. z o.o. or its suppliers as a result of the installation or use of the Software.” No data processed. 100
57	Homestar VR: Special Edition	https://www.pckt.co.jp/privacypolicy.html This policy is presented entirely in Japanese with no English (or other language) option. Google Translate was used to attempt to understand the policy, however it is neither clear nor accessible. It identifies the (very little) data that it collects but there is no attempt to meet any GDPR requirements.
58	Henry	https://www.oculus.com/legal/privacy-policy/ this redirects to https://www.meta.com/ie/legal/privacy-policy/ This is a Meta policy which has been assessed above. Its score has been copied down.
59	Wraith: The Oblivion - Afterlife	https://www.fasttravelgames.com/privacy-policy/ Same as 01 Vampire: The Masquerade – Justice and 35 EverSlaught Invasion
60	Please, Don’t Touch Anything: House Broken	https://forwardxp.com/privacy-policy-please-dont-touch-anything-housebroken/ Does not process personal data

61	Monkey Doo	https://www.clique.games/privacy This policy applies the usual US definition of personal data. It also refers to the Privacy Shield Framework which is no longer valid. Although this policy does advise that it processes data for the performance of a contract, this is under the heading of “Purposes”, rather than legal basis. Performance of a contract does not cover all processing and Legitimate Interests is not present. Rights are incomplete.
62	2MD: VR Football Unleashed ALL STAR	http://truantpixel.com/privacypolicy2020.pdf “We do not collect and store any of your personal information”
63	NFL PRO ERA II	https://www.status.pro/privacy-policy A good, clear, comprehensive policy. Up to date in referencing adequacy decisions and standard contractual clauses in relation to data transfers.
64	Colossal Cave	https://www.colossalcave3d.com/privacy-policy/ “We do not collect anything additional through any VR devices, including the Oculus Quest 2. “
65	Hellsweeper VR	https://vertigo-games.com/privacy-policy/ Same as 10 Time Stall

References

[1] N. Stephenson, *Snow Crash*. United States: Bantam, 1992.

[2] Meta, "Introducing meta: A social technology company," 2021. [Online]. Available: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[3] European Commission, "Guidelines on Data Protection Impact Assessment." [Online]. Available: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

[4] Chayka, Kyle, "Facebook wants us to live in the Metaverse." [Online]. Available: https://www.newyorker.com/culture/infinite-scroll/facebook-wants-us-to-live-in-the-metaverse

[5] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council." [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[6] ——, "Regulation (EU) 2016/679 of the European Parliament and of the Council," Article 5, Principles relating to processing of personal data. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[7] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council," Article 6, Lawfulness of processing. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[8] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council," Article 4, Definitions. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[9] Martin, Baily, "Privacy in a Programmed Platform. How the General Data Protection Regulation applies to the Metaverse," *Harvard Journal of Law & Technology*, vol. 36, no. 1, 2022. [Online]. Available: https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf

[10] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 319–352, 2023.

[11] C. B. Fernandez and P. Hui, "Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse," in *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2022, pp. 272–277.

[12] Y. Canbay, A. Utku, and P. Canbay, "Privacy concerns and measures in metaverse: A review," in *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)*, 2022, pp. 80–85.

[13] Aamir, Omer, "Metaverse and Its Regulation." [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4306357

[14] J. Kim, "Advertising in the metaverse: Research agenda," *Journal of Interactive Advertising*, vol. 21, no. 3, pp. 141–144, 2021. [Online]. Available: https://doi.org/10.1080/15252019.2021.2001273

[15] C. Sandeepa, S. Wang, and M. Liyanage, "Privacy of the metaverse: Current is-

sues, ai attacks, and possible solutions," in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, 2023, pp. 234–241.

[16] P. L. Kharvi, "Security risks, user privacy risks, and a trust framework for the metaverse space," in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, 2023, pp. 119–123.

[17] H. Guo, H.-N. Dai, X. Luo, Z. Zheng, G. Xu, and F. He, "An empirical study on oculus virtual reality applications: Security and privacy perspectives," in *2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE)*, 2024, pp. 1958–1970.

[18] Meta, "Meta quest app store," 2024, accessed on Apr 08, 2024. [Online]. Available: https://www.meta.com/en-gb/experiences/

[19] Meta, "Learn about app privacy data types," Collection of user data by App. [Online]. Available: https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/app-privacy-data-types-meta-quest/

[20] ——, "Developer Data Use Policy," Meta Data Use Policy. [Online]. Available: https://developer.oculus.com/policy/data-use/

[21] Meta, "Privacy policy requirements," Meta Privacy Policy Requirements. [Online]. Available: https://developer.oculus.com/policy/privacy-policy/

[22] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council," Article 28, Processor. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[23] E. Parliament and C. of the European Union, "Regulation (eu) 2016/679 of the european parliament and of the council," Article 26, Joint controllers. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[24] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council," Article 12, Transparent information, communication and modalities for the exercise of the rights of the data subject. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[25] ——, "Regulation (EU) 2016/679 of the European Parliament and of the Council," Article 13, Information to be provided where personal data are collected from the data subject. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[26] E. Parliament and C. of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council," Article 14, Information to be provided where personal data have not been obtained from the data subject. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[27] PEGI, "PEGI age ratings." [Online]. Available: https://pegi.info/page/pegi-age-ratings

[28] ——, "What do the labels mean?" [Online]. Available: https://pegi.info/what-do-the-labels-mean

[29] DLA Piper, "DLA Piper — Data Protection Laws of the World." [Online]. Available: https://iapp.org/resources/article/dla-piper-data-protection-laws-of-the-world/

[30] Meta, "Supplemental Meta Platforms Technologies Privacy Policy." [Online]. Available: https://www.meta.com/ie/legal/privacy-policy/

[31] ——, "Hand and Body Privacy Notice." [Online]. Available: https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/hand-tracking-privacy-notice/

[32] ——, "Eye Tracking Privacy Notice." [Online]. Available: https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/

[33] ——, "Natural Facial Expressions Privacy Notice." [Online]. Available: https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/natural-facial-expressions-privacy-notice/

[34] ——, "Fit Adjustment Privacy Notice." [Online]. Available: https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/fit-adjustment-privacy-notice/