Privacy and Data Protection in Mobile Applications

Tselekidis Dimitrios
SID: 3307190018

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Cybersecurity

JANUARY 2022
THESSALONIKI – GREECE
Privacy and Data Protection in Mobile Applications

Tselekidis Dimitrios

SID: 3307190018

Supervisor: Prof. Komnios Komninos
Supervising Committee Members: Assoc. Prof. Name Surname
Assist. Prof. Name Surname

SCHOOL OF SCIENCE & TECHNOLOGY
A thesis submitted for the degree of
Master of Science (MSc) in Information and Communication Systems

JANUARY 2022
THESSALONIKI – GREECE
Abstract

In a world where the industry of mobile applications is continuously expanding, privacy is a major concern for the consumers. When end-users utilize applications, many of their personal data are handled by all the actors in an application ecosystem. General Data Protection Regulation arises as a solution to privacy issues in the European Union. However, the majority of the applications are lacking in security and compliance when dealing with information which result in severe problems. This article presents the key points of privacy, data protection, and the GDPR about mobile applications and pinpoints the most usual weaknesses. An informed guide with information about privacy-preserving techniques and their implementation in application development has been created. This paper will complement other researches about privacy and data protection in mobile applications and could raise concerns for users, application developers and researchers.

Tselekidis Dimitrios

28/1/2022
Preface

This dissertation is written as the final part of a Master’s degree at the International Hellenic University in the faculty of school of science and technology. The work was carried out from July 2021 to January 2022. Guidance and supervision was performed by Prof. Komninos Komnios.

The topic under discussion is of high relevance for any organization or other body that is concerned about processing of personal data by smartphone applications. Especially the purposes and means of data collection and the measures of data protection in mobile applications.
# CONTENTS

Abstract ................................................................................................................................. -v-

Contents ................................................................................................................................. -v-

Introduction ............................................................................................................................ -1-

1. What is Privacy? .................................................................................................................. - 3 -
   1.2 Location privacy ........................................................................................................... - 8 -
   1.3 Trust ........................................................................................................................... - 9 -
   1.4 Problems are arising ................................................................................................... - 9 -
   1.5 Revenge pornography .................................................................................................. - 10 -
   1.6 More challenges .......................................................................................................... - 12 -
   1.7 How to protect privacy ............................................................................................... - 13 -
   1.8 Privacy by design ....................................................................................................... - 14 -

2. Data protection and GDPR in smartphone applications .................................................. - 17 -
   2.1 Data protection as a right ............................................................................................ - 17 -
   2.2 GDPR ....................................................................................................................... - 18 -
   2.3 What is personal data ............................................................................................... - 21 -
   2.4 Consent ..................................................................................................................... - 22 -
   2.5 Article 32, Security of Processing ............................................................................. - 23 -
   2.6 Right to be Forgotten ............................................................................................... - 24 -
   2.7 Right to Access ......................................................................................................... - 25 -
   2.8 DPIA .......................................................................................................................... - 26 -
   2.9 E-privacy Regulation ............................................................................................... - 28 -

3. Smartphone Ecosystem and actors involved .................................................................... - 31 -
   3.1 Smartphone Ecosystem .............................................................................................. - 31 -
   3.2 Apps ............................................................................................................................ - 32 -
   3.3 Permissions ................................................................................................................ - 32 -
   3.4 Operating system providers ...................................................................................... - 35 -
   3.5 Users ........................................................................................................................... - 36 -
   3.6 Network Communications ......................................................................................... - 36 -
   3.7 Unique Identifiers ..................................................................................................... - 37 -
4. Compliance and Data Protection Challenges .................................................. - 40 -

4.1 Cross border Transfers .............................................................................. - 40 -
4.2 Risk data practices of Developers ............................................................... - 41 -
4.3 Application Stores ..................................................................................... - 44 -
4.4 Contact tracing apps during the Covid-19 .................................................. - 45 -
4.5 Transparency .............................................................................................. - 46 -
4.6 Right to portability ..................................................................................... - 47 -
4.7 Profiling ..................................................................................................... - 47 -
4.8 Rights and obligations regarding children .................................................. - 48 -
4.9 Embedded sensors on mobile devices ........................................................ - 48 -
4.10 Third-party sharing ................................................................................... - 49 -
4.11 Third-party content ................................................................................... - 49 -
4.12 Data retention ........................................................................................... - 50 -
4.13 Privacy policies ........................................................................................ - 50 -
4.14 Consent ..................................................................................................... - 52 -
4.15 Use of untrusted Content .......................................................................... - 52 -
4.16 Authentication .......................................................................................... - 53 -
4.17 Privacy ..................................................................................................... - 53 -
4.18 Supply chain ............................................................................................. - 53 -
4.19 Transmission ............................................................................................. - 54 -
4.20 Permissions ............................................................................................... - 54 -
4.21 End-User ................................................................................................... - 56 -
4.22 The role of users and consent. Pre-installed software ............................... - 57 -
4.23 Storage ...................................................................................................... - 58 -
4.24 IN-APP payments .................................................................................... - 58 -
4.25 Mobile application security threats ............................................................ - 59 -
4.26 Use of untrusted applications ................................................................... - 60 -
4.27 Location-based mobile applications (LBMA) ............................................ - 60 -
4.28 Application handling ................................................................................ - 61 -
4.29 Big Data ................................................................................................... - 62 -
4.30 Artificial Intelligence and Smart homes. ................................................... - 65 -
5. **Application improvement** .......................................................................................... - 67 -

5.1 Data literacy ............................................................................................................. - 67 -
5.2 Privacy policies ....................................................................................................... - 70 -
5.3 Consent ....................................................................................................................... - 73 -
5.4 Mobile security best practices .................................................................................. - 73 -
5.5 Secure payment ......................................................................................................... - 75 -
5.6 Application Developers ............................................................................................ - 76 -
5.6.1 Permissions best practices .................................................................................... - 78 -
5.6.2 Automatic decision making .................................................................................. - 79 -
5.6.3 Storage limitation .................................................................................................. - 79 -
5.6.4 The right to erasure ............................................................................................. - 79 -
5.6.5 Data transmission .................................................................................................. - 79 -
5.6.6 Cross border transfers .......................................................................................... - 80 -
5.6.7 Data portability ...................................................................................................... - 81 -
5.6.8 Third-party code. ................................................................................................... - 81 -
5.6.9 Data storage ........................................................................................................... - 81 -
5.6.10 Children ............................................................................................................... - 83 -
5.6.11 Accountability ...................................................................................................... - 83 -
5.7 How can app stores enhance privacy and data protection? .................................... - 85 -
5.8 Privacy by design ........................................................................................................ - 87 -
5.9 Regulations ................................................................................................................ - 90 -
5.10 Automation tools ...................................................................................................... - 91 -

6. **Conclusions** ........................................................................................................... - 93 -

7. **Bibliography** .......................................................................................................... - 96 -
Introduction

Nowadays smartphones are the most ubiquitous devices in the world. From toddlers until people in later life almost everyone uses a smartphone in many aspects of his/her life. Smartphone applications are one of the most prolific industries releasing millions of applications every year that help people have fun, socialize and even assist in work-related activities. By having the smartphone constantly near us and spending a large portion of the day in applications and services a lot of personal information and sensitive data is collected and processed by applications. Even if we voluntarily disclose and provide some of this information applications are responsible for a wide range of activities that put individuals’ privacy into risk. People are constantly in a trade-off between privacy and smartphone applications usability and in many cases without even realizing it. Regulations and policies have been implemented, with the GDPR in Europe making a difference but still there are many risks. The protection of personal data is a fundamental right and many measures have been proposed and put into effect in order to enforce data protection. However there are many mismatches between the law and how it is actually transferred into technology matters. Furthermore the average users but even developers lack the understanding and knowledge to make informed choices. In this paper we will analyze the privacy and data protection concepts regarding smartphone applications.

Research Goal
The goals of this dissertation are to understand how privacy and data protection is affected by smartphone applications. Further, to highlight the most common data protection and GDPR compliance risks and check how compliant applications are. Moreover, to identify the best ways to improve applications by enhancing their GDPR compliance and data protection. To achieve our goal will require knowledge of the GDPR and how the legal requirements can be translated into technical solutions while search for additional ways to protect personal data in the smartphone ecosystem.
Research Method

Our research was based on literary review analysis. Online sources were used consisting of legal documents and scientific researches. Due to technology related subject we focused on recent studies (5 years) to address concerns for the current state of mobile applications.

Outline

The remainder of the thesis is structured as follows:

Chapter 1 introduces the term of privacy and its rights. Further, it explains some challenges regarding privacy and new technologies and steps that are taken to preserve privacy.

Chapter 2 introduces the data protection and GDPR regulation and how they relate to mobile applications.

Chapter 3 explains the smartphone ecosystem and all the actors involved in the application lifecycle.

Chapter 4 explains the most common challenges and risks regarding security and data protection of mobile applications covering a wide range of different aspects.

Chapter 5 suggests best practices and ways to implement security and privacy preserving measures in order to avoid privacy risks when we are using services of smartphone applications.

Conclusion presents concluding remarks and proposals for future work.
1. What is Privacy?

In this section, we discuss the technical and historical background of the term privacy. There is a brief introduction of the term and its connection with new technologies. There is also a discussion about some current challenges that have emerged with the use of technological devices and ways to preserve our privacy in this new era.

Privacy is a right of every human and almost as old as the existence of humanity, but it was not always legally protected. Moreover, how could it be since there is a significant difference between what is considered private and what is legally protected as private. In our days, privacy and data protection are protected by regulations and laws but still are being threatened more than ever. Smartphones, social media, IoT, drones, biometrics, the Internet, and many more innovations come out so fast that it is almost obsolete when a new regulation is created. So the last decades, with the revolutionary advance of science and technology, it became much easier to intrude on someone's privacy.

Monitoring existed for years, especially in small communities where the neighbors were watching and, in this way, enforced the moral norms of the given community. Nowadays, we are not only being watched by a far greater crowd, but all the information is sometimes stored even without limits of the amount of data, the reason, and the duration. It is also much easier to transfer and organize this information, which can considerably impact our lives. We have reached a stage where someone can have a complete life online (working, dating, shopping) and is being identified as individual only by the information and data she/he provides.

Technology plays an important role and should be always taken into consideration when a new regulation comes out that a correlation with the privacy of the people.¹

The concept of privacy in the eyes of the law appeared for the first time in an article in Harvard Law Review in 1890, where Brandeis and Warren mentioned the right to privacy,

¹ A. Lukács, “What is privacy? The history and definition of privacy ” p. 10.
the right to be let alone, and the need to take legal action in order to protect the rights and
the individuals by the recent inventions, which referred to the widespread use of
photography and newspaper. The Cambridge dictionary defines privacy as "someone's right
to keep their personal matters and relationships secret and the right to be alone and do
things without other people seeing or hearing you." We can understand by the definitions
that privacy is a right without clear definition but tries to protect against unwanted
disclosure of private facts like thoughts, emotions and how, when, and for how long this
personal information can be communicated by others.

With the extensive use of smartphones and their applications, it has become relatively easy
to gather, store and share all this information. While on the same time, it is almost
impossible to protect all the information that others can have access to.

What information is sensitive and private? In the eyes of the law, personal data that are
acquired by surveillance or a malicious way and uncovering someone's private world is not
legal. However, there arises a new problem since this paradigm heavily influences the law.
What happens when this information is not secret? In some legal orders, the courts
conclude that since something is not secret, it cannot be private. And there, we have
victims of revenge porn, personal information leaked by social applications, etc.

Privacy is also a social concept we were taught during our life. We have a lot of different
relationships, friends, acquaintances, and family, which can be formal and informal. When
we share some of our information, we rely on the expectation about what is going to
happen with this information based on the level of intimacy and trust we have with each
social group. The problem is that the same thinking cannot be applied to technology-related
disclosures. For example, when we decide to download an app and provide our personal
information, we share it with the expectation that it will be used solely for our specific
purpose. Most of the time, this is not what is happening. So it is critical to change our

2 M. Furini, S. Mirri, M. Montangero, and C. Prandi, “Privacy Perception when Using Smartphone
Z.

3 D.J Solove, “The digital person: technology and privacy in the information age,” Choice Reviews Online,
perspective on privacy. What we share, with whom, and how we share it plays a significant role in what can be private and what is not. In the "Tastes, Ties and Time" project where a lot of personal information of students leaked although the researches had privacy in mind, there was improper access to personal information. Subjects had used Facebook's options to restrict access to their information to the whole world and allow only their friends to access them. But being in the same network as "friends," the researchers had access to this information and considered them freely accessible for research.

Even something we do not consider private can lead to privacy implications and risks. For example, the battery status API is used by websites to check a device's battery levels. Because this information has a minimal impact, it does not require any permission from the user. But by using this information in a corporate environment where devices share similar settings, it is possible to distinguish devices and therefore recognize a specific user.

People usually do not object to sharing information with others, even sensitive ones. For example, patients share information with doctors about their health because there are norms that dictate how much information and what type are fitting in each occasion. Not every information should be considered as private because it takes place only inside our home. When we talk in a restaurant or on the train, we expect not to be listened to as we expect privacy in almost all public places. So even if the disclosure is a violation of privacy, avoiding disclosure does not mean is the only way to protect it.

Nowadays, databases hold a lot of information that people have no control over them. Although this information might not be so sensitive, like daily activities, Facebook status,

---


5 M. Zimmer, “‘But the data is already public’: on the ethics of research in Facebook,” *Ethics Inf Technol*, vol. 12, no. 4, pp. 313–325, Dec. 2010, doi: 10.1007/s10676-010-9227-5.


or music preferences, individuals are more comfortable of sharing all this information on their smartphones than health or financial data. But still how all this information is used, by whom and for what reason is problematic.

In the last 40 years, there have been many formulations of privacy principles, but most of them were regarding information privacy or data protection. However, as shown, some other privacy principles are not addressed or taken into account and this negligence could have harmful results. As we previously stated, to take defensive measures and protect privacy, we first need to identify the categories and types of privacy. All these types of privacy are related to the individual's space, internal and external, his or her functioning within that space, and the relationship with others.

- **Privacy of personal information** which is also referred to as data and information privacy. Individuals do not want their data to be available to others. Even when this data is possessed by another party, the individual should be able to control the data and its use.

- **Privacy of the person or body privacy** which is referred to an individual body. It could be explained as freedom from torture and the right to medication, which are human rights, including body searches, blood transfusion without consent, compulsory immunization, and submission to biometric measurement.

- **Privacy of personal behavior** which refers to the observation of what an individual does, sexual preferences, political or religious practices.

- **Privacy of personal communications** which refers to analyzing or recording communications, the use of spying bugs. Individuals desire to communicate freely with others without the fear of monitoring.

---


• **Privacy of location** refers to the right of an individual to be present in a location or space without being tracked and anyone knowing where he or she is. Space can also be physical or cyberspace.

• **Privacy of thoughts and feelings** is the counterpart of body privacy. It is also called decisional privacy, for example, to give women the right to make decisions regarding their bodies or terminate a pregnancy.

• **Privacy of association** includes social and political relationships formed by people.

These aspects are trying to include the privacy impacts of the new arising technologies in order to protect an individual's rights and freedoms successfully. From these aspects, we can achieve better proactive protection. It may be beneficial for policymakers who will gain a better understanding of privacy and acquire the knowledge to protect it in the future despite the emerging technological developments.

Information privacy is being diminished day after day from new rising technologies. People decide what data is willing to reveal, and his/her concept of privacy is changeable depending on the expected benefit someone has to gain for revealing his/her information.

The perception of personal privacy is different in different cultures around the world. Something that is considered personal in one country maybe is considered acceptable for sharing in another.\(^\text{12}\) For example, in the culture of Japan existed public baths which allowed strangers to naked bath side by side, and even if it was officially forbidden, mixed-bathing has survived for many years especially in rural areas. Furthermore, in Japan, every member of a household owns his or her specific chopsticks and bowl when in the U.S, all members of a household can access every utensil they like. So we can understand that specific contexts of privacy may be vary depending on the place someone is in the world, and for that specific reason, it is of great importance to develop a rich sense of what privacy is so we could be able to protect it in the new interconnected world of Internet.\(^\text{13}\)

---


User perception about privacy is also influenced by their personality traits and trust. Some users who have lower personal trust may not want to share their information with others, however they are not covered by the default settings of a smartphone and should take additional measures.14

Sociality has taken an expense on our privacy. Sociality always required some abandonment of our privacy, leaving our home, or sharing our time and secrets with others, but a balance always existed. Nevertheless, with the rise of social networks has changed the way we manage our relationships. The broader use of these networks can help to the collapse of personal and professional contexts. In addition, in such an environment where for someone to be social is demanding to share information, it can be quite concerning for our privacy.15

1.2 Location privacy

Location privacy is the ability of a person to move in every public space and that under normal circumstances, their position will not be recorded or stored for any type of water usage.16

To avoid the misuse of our location privacy while we take advantage of the positive impacts, we can use protections models like location hiding, the anonymization of users, and cloaked regions. In this example, tourists will be able to get suggestions and


recommendations about what places to visit, restaurants, tours, etc. without compromising their privacy regarding their locational information.17

1.3 Trust

Privacy plays a significant role even in information relationships and for these relationships to thrive, trust is imperative. Trust-promoting privacy rules by companies will allow people to feel safer to disclose their information, and that will benefit both the individuals and the companies. Privacy can help to promote trust and become essential to our digital future. Trust presupposes a person will become vulnerable to another person or to an organization. Vulnerable means that the information shared can be misused, manipulated, or shared; unlimited possibilities for disclosure exist. However, having trust can form safe and long-term relationships with entities that promote clients' privacy18. Moreover, this can be a crucial point for people to gain a choice and improve the privacy standards of many companies. This can be achieved if businesses understand how much customers value their personal data and, after this, adopt privacy-protective strategies that will become a competitive advantage for their business.19 After all, many individuals frequently take privacy-related decisions.

1.4 Problems are arising.

With the mobility that derives from the use of mobile phones and their applications, new privacy concerns emerge in different environments. Social media platforms which by nature require some information disclosure by the users, are being used every day and have become a requirement for genuine world sociability. We can understand this by thinking of how many times we searched for a new acquaintance online. Furthermore, an online profile without the latest or sufficient information could negatively impact and even be stigmatized.

by the new age norms resulting in isolation in real life. It is easy to understand that many young users are forced to exchange some of their privacy on social media platforms in order to satisfy their inherently social needs in real life.\textsuperscript{20}

Privacy policies are the best tool we have to understand how companies use our data. The problem is that policies, most of the time, are too long for someone to read, are very difficult to understand, and sometimes are ambiguous on critical terms. This results in people having difficult times deciphering the language and what is said between the lines. Even knowledgeable users have great difficulty understanding the true meaning of a policy. \textsuperscript{21} Additionally, even experts in the field disagree on the meaning of some key terms. It becomes clear that an average user will face many obstacles to understanding privacy policy.

Furthermore, for the same reason, users read a policy once per year and then go on with their business. This can drive people to care less about policies and privacy threats. For example, if a user cares only about his credit card information and visits a site that states that it does not collect or store credit card info, the user might feel it is ok to use it even though it is quite possible that at the same time a lot of other personal data is being used.\textsuperscript{22}

\textbf{1.5 Revenge pornography}

Consensual sharing of naked images is done with the understanding that these images will remain confidential and only for their partner's eyes. Most of the times sharing occurs only after the assurance of the partner. Nowadays, with the click of the mouse, it is easy to see such photos or videos that have been taken only because someone who is trusted asked and assured that it would be kept private. However, there are cases that users does not understand that consent into one context, which is a relationship, does not mean consent in other contexts like sharing personal data with the whole world. This contextual nature of


\textsuperscript{22} A. M. McDonald and L. F. Cranor, “The Cost of Reading Privacy Policies,” 2009 p. 22.
consent plays a vital role in information privacy. Policymakers have recognized the importance of context, but even everyday people intuitively understand the meaning of context; for example, when sharing health data with our doctor, we are sure that all of our data will remain private, or when we are giving our credit card in a restaurant we do not consent to the use our card for personal purchases\textsuperscript{23}. It is of great importance to understand that using data that is shared for a specific purpose into another context should be considered illegal and a privacy violation.\textsuperscript{24} Most of the time, videos and photos with sexual content were published online by disappointed and vengeful ex-partners and even if the "actors" have consented in the recording they have not to consent to share it in public. Revenge pornography is called as a severe sexual offense with the use of technology, but we need to keep in mind that it is also an attack on privacy and the right to a good name; that is the reason it is not taken as seriously in Europe as in other countries, because privacy even as a fundamental right and a protected value has different criminal codes from a sexual offense. However, revenge pornography compromises many aspects of an individual's life, such as his/her physiological state, sexual identity, and expression that can be assessed as a sexual offense.\textsuperscript{25} It is imperative to have a new criminal law definition in order to combat this new cybercrime and have most serious and severe legislation and approach.

Revenge pornography is also called cyber-harassment and has effects not only on the psychological and social health of a victim but also damages the core of our society. Most of the harassment is happening against women or members of the LGBTQ community, people being discriminated against. It can also be called a breach of trust because all the personal data that was shared was with people of the inner social circle of the victims who had gained their trust, and it is a common belief that this information will be kept confidential. The main problem is the nature of the Internet; with one image posted, the uploader loses control of what will happen how this image will be used. Most of the time,


the uploader can be identified, and even if he is or she is brought to justice, it is almost impossible to stop the sharing of the image.26

1.6 More challenges.

With the rise of IoT home devices, even the sanctuary of our home can pose a threat to our privacy. Home monitoring technologies can upgrade our living standards at a low cost. Especially for seniors who are more prone to downgrade their privacy in order to receive the benefits of safety and home monitoring technology inside their home. 27Home devices are valued by older individuals because they allow them to age in their place instead of searching for help in other choices, which can be far more expensive like centers of eldercare.

Privacy professionals and other personnel related to privacy rarely take place in the designing phase of an app or a product and do not communicate enough with the engineers and programmers. Even on larger companies that presumably take privacy into solid consideration, there were problems with prioritization, and as usual, privacy is not a top priority for engineers. Additionally, for engineers having more data is really helpful to improve their work so that privacy can be an obstacle on their way to a more functional result. Besides the above, privacy it is not easily enumerated, so it can be easily opted out when there is a strive for success and limited time to achieve it.28

Another significant vulnerability for privacy is the human tendency to trust. Users tend to trust other humans easily, especially strangers or strangers posing as trustworthy people (phishing attacks). In addition to phishing, social engineer poses a significant threat and exploits human psychology at first and then a company's systems. The way to reduce human vulnerabilities in an organization may be one of the most cost-effective in

proportion between the increase in security and the money spent. This can derive from adequate training and education about cyber awareness and cyber hygiene.\textsuperscript{29}

Another trend implemented by tech companies is BYOD (bring your own device) at work and use it. With this policy, personal and work data are stored in the same device, which most of the time does not have trust features or have been rooted, transforming them into a possible threat. Organizations should assume that all of these devices can be malicious and treat them as such. They should secure them correctly and monitor their security continuously, something that it is possible only when they are being used for work-related reasons. Except for the apparent strategy of restricting BYOD policies, organizations can fully secure each device and, if there is a deviation of this state, be detected and have a quick response. Furthermore, using an isolated sandbox container or device integrity applications can help improve the trust in BYOD devices.\textsuperscript{30}

\textbf{1.7 How to protect privacy.}

In our society, privacy can be protected by mainly three mechanisms. Legal regulations, ethical self-regulation, and technologies that help promote privacy. Nowadays, there is specific legal protection for privacy but with different extend and range depending on the place of the world. Ethical self-regulation can be pretty effective even if it cannot pose sanctions such the legal regulations. Professional discretion and confidentiality allow the sharing of personal information depending on the context. Individuals also can use technology to protect their privacy. Privacy protecting-apps, consent and permissions, and data encryption or anonymization can help achieve a better and more protected privacy environment.\textsuperscript{31}


The contextual definition of privacy is important and it is critical to clarify who receives the information, what type of information it is, how it is used, for what purpose, and in what context. The privacy expectations in mobile devices depend on the context of exchange. For example, we decide to exchange our location privacy in order to have better navigation or share some personal information and photos for social networking. The problems arise when the above information is used in different contexts, for example our location privacy to be used for advertisements or tracking without notice.\(^{32}\)

It is crucial to make informed choices regarding our privacy when buying a product before a breach occurs. In this way, we participate in forcing companies to make products with the consumer privacy in their mindset.

### 1.8 Privacy by design

In the EU Charter of Fundamental Rights, privacy is shared between two protected rights, the right to respect an individual’s private life, home, and communications and the right of the protection of personal data. These two articles (7 and 8) describe the rights as independent, but they can also be complementary to each other or even have some clashes with one another. For example, while non-repudiation is really important and critical for data protection, it can cause problems in confidential communications because it disrupts confidentiality by canceling the plausible denial. Furthermore, some clashes may exist in the same right; for example, plausible deniability can be of high importance for the sensitive data, but it has problems with the other attributes of the right.\(^{33}\) Data processing is happening everywhere, in business, in government, and in private life and for the processing of data computers are used. Computers use software that is instructions on how to operate, and these instructions must comply with the legislation regarding privacy. So


privacy can be largely dependent on the design of software which is highly dependent on the knowledge and the interest in the privacy of the developer. So we can understand that privacy by design essentially means to embed privacy into information technologies, business practices, and networked infrastructures as a core function.\textsuperscript{34}

As it is already stated, in order to achieve privacy by design, it is important to have two types of knowledge, legal knowledge about privacy and knowledge of software development. Both types should be implemented during the development of a new software and take in mind the architecture, the data design, the process design, and the interface design.\textsuperscript{35}

There are seven foundational Principles of Privacy by Design which are the core of a framework on how to implement privacy by design in the new technologies as described in the book of A. Cavoukian\textsuperscript{36} and will be discussed in detail below.

The first principle is called \textit{Proactive, not Reactive}, and it is easy to understand that it has to do with the prevention of incidents before they occur.

The second principle is called \textit{Privacy as a Default Setting}, and it is the means that can protect an individual's privacy even if the individual does nothing. The data is still protected by the system by default.

The third principle is called \textit{Privacy Embedded in Design}, and it points out how important it is to embed privacy as an essential component into the architecture and not add later; this way, privacy is considered an essential function and works with all the functionalities of a system.

The fourth principle is called *Full functionality, Positive Sum*, and it describes the way Privacy should be implemented without making trade-offs for security or speed of an application, demonstrating that it is possible to achieve all of these functionalities at the same time.

The fifth principle is called *End-to-End Security* and aims to provide protection in the entire lifecycle of the data, from the start till the end. It ensures that all information is securely stored, accessed and processed, and then destroyed in the time required.

The sixth principle is called *Visibility and Transparency* and assures everyone (from users to providers interested) that everything is operating as it should be, and the well function is visible and transparent.

The seventh principle is called *Respect for User Privacy- Keep it User-Centric*, and it shows that architects should have the interests of the users in mind by implementing measures such as privacy defaults, notices, and user-friendly options.
2. Data protection and GDPR in smartphone applications

In this section, we discuss the data protection principles, and we analyze the General Data Protection Regulation regarding smartphone applications. The E-privacy Regulation is also presented, and the outcomes for applications of its implementation are discussed.

Data protection is a legal framework that has evolved as a tool of privacy over the internet and continues to evolve and change. It is used to protect individuals’ personal data online, strike a balance between fair and proper use of information, and enable trade between states. It is the implementation of appropriate, administrative, technical, or physical measures to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data. It also ensures the fair processing of personal data by public and private sectors while protecting any information related to an identified or identifiable living person. Both privacy and data protection are two fundamental rights in the EU.

2.1 Data protection as a right is meant to be used as an enabler for a broad range of other rights and privacy amongst them, so it is said that data protection right exist to serve other rights and not to represent any value or interest. Although it may not represent any value, its procedural nature is verified. Data protection maybe be the answer between the controllers of data processing and the individuals whose data are being used and are in need of protection which has risen from the advances in computing technologies and the new roles they have acquired in our society. By ascending data protection as a fundamental right, it helped to differentiate it from privacy while at the same time creating an instrument that can be responsive to society's ever-changing needs and provide the level of protection it is required.

37 International Organisation for Standardisation/IEC 2382–1-1993
2.2 GDPR
The GDPR is a compilation of mandatory provisions adopted by the European Parliament, the Council of the European Union, and the European Commission to regulate information issues in EU territory. The regulation has applications to the collection, retention, and transfer of private individuals' personal data and establishes rules for the protection of privacy. The GDPR is the most up-to-date regulation which replaced the various directives of member states and provided a unified data protection framework that is legally bound to implement by all members of the EU, thus creating a trust that can help the digital economy to thrive across the internal and the external markets.

GDPR is an important data and privacy law from the European Union, but it has a global influence. Its application is required to mobile apps that collect and process personal data of EU citizens even if an application is operated outside the EU.

From a technical view, GDPR protects and secures data when they are stored or transferred, control who has access and can monitor them, and at last, tries to detect a breach as soon as possible.

Under the GDPR, three data protection roles are defined:

- The data subject, a natural person whose information is being processed.
- The data controller is a natural or legal person who decides the purpose and means of processing data.
- The data processor can be either a natural or a legal person and is the one responsible for carrying out the processing of a subject's personal data on behalf of a data controller.

Lastly, there is also the Data Protection supervisory Authority which is an independent authority established from each European Member State and contributes to the application of GDPR principles by investigating, correcting, and issuing fines. Except from the above, the DPA regulates the processors and controllers in its own state.
Seven principles of GDPR

1. ‘Lawfulness, fairness, and transparency’: When someone processes personal data shall have a legitimate ground like consent to do so (lawfulness). Fairness and transparency towards the data subject are a requirement for processing personal data while being clear, honest, and not withholding any information regarding who you are and the purpose of collecting and using data and acting fairly towards data subjects.

2. ‘Purpose limitation’: When an app processes or collects personal data, the app needs to have specified, explicit and legitimate purposes for doing so, must inform the data subject, and not process any further if the above purposes are voided. Further processing for other purposes is only allowed on the basis of a specific set of criteria in the GDPR (Article 6(4)).

3. ‘Data minimization’: Personal data need to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4. ‘Accuracy’: Personal data shall be accurate and, where necessary, kept up to date. In addition, every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay, having regard to the purposes for which they are processed.

5. ‘Storage limitation’: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for more extended periods only if specific criteria exist.

6. 'Integrity and confidentiality': Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. In view of this, data controllers shall implement appropriate technical or organizational measures.

---

7. “Accountability”: The controller needs to demonstrate appropriate measures and records of them as proof of compliance with the GDPR principles.

Besides the above, GDPR implemented some new rights for data subjects, such as the Right to data portability (Article 20)\(^{41}\) which makes sure that an individual’s data is in a format that can be used from a machine and can be transmitted to another controller whenever it is required. Another two rights that were introduced with the GDPR are the Right to withdraw consent (Article 7(3))\(^{42}\) and the Right to be Forgotten (Article 17).\(^ {43}\)

The framing of data protection as a right by the GDPR has imposed a lot of obligations for companies and private individuals who are developing a product. There are many things that the developers must take into account before creating and selling something.

Although data protection was always tied to privacy, at the beginning of the 90s, the EU had the inception of the development of data protection law which was legally accepted as a standalone right. A regulatory package that was proposed the same year included the Data Protection Directive (DPD), which was critical for the conception and implementation of GDPR. In the EU’s fundamental rights catalog, there is a distinction between the right to privacy (article 7) and the Right to data protection (article 8). Due to the importance of transferring data into different countries in order for the business to become more profitable, data protection started to acquire a more international principle and somehow distinguish it from the Right to private life.\(^ {44}\) It is important to note that GDPR is a regulation in contrast to a directive, so it became an enforceable law in all member states and helped to harmonize the data protection laws in the EU. This helped and provided better data protection rights and, of course, new business opportunities. The GDPR has

\(^{41}\) General Data Protection Regulation 2016/679, Article 20
\(^{42}\) General Data Protection Regulation 2016/679, Article 7.3
forced organizations outside the EU to comply with its requirements if they conduct business with the EU since there are huge fines and compensations, damage to the reputation if a non-compliance occurs. By doing, so GDPR protects the data of European citizens everywhere in the world.

2.3 What is personal data.
The definition of personal data is broad “any information relating to an identified or identifiable natural person (data subject).”\textsuperscript{45} Identifiable is a natural person who can be identified by reference to an identifier such as a name. Personal data are being collected and used for numerous reasons like improving performance and safety. It can also be used for commercial and money-making reasons.

Personal data are information about a person which can take many forms (numeric, images) and can be objective information like a name, identification and subjective information like opinions, beliefs, etc. But in order to consider personal data, they also need to be relevant, which means that information has meaning and is valuable. Insignificant information should not be considered as personal data. However, that requires further consideration due to new technologies like big data and AI being able to synthesize a lot of irrelevant and insignificant information into data that can be considered as of value.

So in order to understand if some kind of data can be characterized as personal data, most of the time requires analysis with taking into consideration the specific context in which the processing of the information happened. In our smartphones, from the nature of the device itself, which is considered personal, all the data that are stored on the device like pictures, emails, contacts are considered private. Furthermore, even data that are related to identifying the device, such as IMEI, location, and logs, and usage of apps, are qualified as personal data, and once they are collected, they fall into the category of data protection framework. This framework does not apply when all the data are being anonymized.

\textsuperscript{45}European Commission, Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016
Anonymized data are data that have erased all information which could lead to the identification of a person if a reasonable effort is exercised. Even stricter requirements apply for access to sensitive categories of data like ethnicity, political and sexual orientation, and health data. Moreover, when an app has access to this kind of data, it has to ensure that it has taken the explicit consent of the user to process the data but only for a specific purpose.

_Pseudonymized data_ are data where personal identifiers have been replaced by a pseudonym, and thus making data unidentifiable but suitable for data processing. Pseudonymization is used to protect personal data by using tokenization or encryption. With pseudonymization, data can be re-identify with the right key if someone has the authority to access that information.

Personal data are described as a new asset since they can create added value for companies that provide services that would be unable to do so without it. They have a commercial value that can be exploited and can result in less privacy and protection.

Nevertheless, all this consciously given information can facilitate some metadata that users are unaware of.

### 2.4 Consent

The concept of consent is of utmost importance in data protection. Consent is the legal basis data subjects offer to a data controller in order to collect and use their personal data after the controller or the processor has demonstrated lawful reasons for such kind of collection and processing.

“Consent should be given by a clear and affirmative act establishing a freely given, specific, informed and unambiguous indication of data subjects agreement to the processing of personal data relating to him or her”

The types of consent are the following:

- Valid consent


• **Free consent**

Freely given consent means that the data subject is not forced to consent in unnecessary data processing in order to acquire a service and be in a different place of terms and conditions acceptance. In a bundling, situation consent is considered not freely given and can lead to invalidation.

• **Informed consent**

The data subject should be informed before making a choice. Elements like the controller's identity, the purpose of processing, what data are going to be collected are some of the essential elements before providing an informed consent.

• **Specific consent**

It is required in situations where data protection risk will emerge if a lot of control over special categories of personal data is required and for the transfer of personal data to other countries.48

• **Children consent**

In order to process data of children of age at least 16 years old, explicit consent is required. Otherwise, reasonable efforts should be made to verify that a parent gives the consent.49

Furthermore, except for the above, an affirmation action like typing a letter must occur.50

### 2.5 Article 32, Security of Processing.

Article 32 of GDPR addresses the nature of security related to the processing of personal data. In this article, no technical requirements are addressed with the intention to be a timeless document and be able to transfer and adapt to new and future technologies. Paragraphs 1,2 state that the controllers and processors must ensure an ongoing

---

48 General Data Protection Regulation 2016/679, Article 49 (1)(a)
confidentiality, integrity availability, and resilience of processing systems while assessing the appropriate level of security regarding the potential risk. This implies that data controllers and processors must keep their systems updated and continuously assess the risk related to personal data leakage and the consequences it might have for the data subject.

2.6 Right to be Forgotten
The Right to be Forgotten derived after a case in Spain vs. Google. According to this, personal data must be erased immediately when they are no longer needed for the original processing purpose, if there is no other legal ground and if the data subject withdraws its consent.

Modern computers and the cloud industry provide us with ample storage capacity and the possibility to store everything and never forget it. If we add intelligent search engines and the use of Big Data and AI technologies to gather online information, someone can easily acquire large quantities of personal information that can reflect with many details the past life of an individual. All this information from scattered and forgettable is becoming permanent and searchable, resulting in threats over someone's reputation with devastating consequences. There are cases where people lost their jobs or acceptance to a university due to a Facebook photo or a status.

This Right was introduced in Article 17 of the GDPR, and its implication gives the opportunity to delete data from all possible sources in which they are stored by giving the Right to a person to ask the data controller for the deletion of his or her personal data. Furthermore, it also allows a person to withdraw consent from an original controller, and then all data controllers who are processing data are forced to delete the information. This can create technical issues because controllers should know all the third parties which process the same data; they should also inform them about the erasure. Additionally, all the information should be tracked in order to be found and then provide proof that it was efficiently removed. All this is technologically questionable due to its technical difficulties, and the enforcement of the Right may be doubted. The Right to be forgotten is a well-intentioned regulation that can help to the protection of personal data; however, there is a problem between the law and technical realities because it is challenging to implement.

---

51 Court of Justice of the European Union (2014) C-131/12 Google Spain SL, Google Inc v. Agencia Española de Protección de Datos(AEPD), Mario Costeja González
legal requirements in systems that have different understandings of concepts like memory and forgetting. Databases and machines can be easily restored to previous states because they have detailed records of these states, and in AI applications, previous information is vital for usability. Since technologies like artificial intelligence are rapidly growing and developing, it is vital to bridge the gaps between law and technology in order to be able to protect the Right to be forgotten in all the aspects and to be seen from different aspects than the human conception of how human memory and the ability to forget function.\textsuperscript{52}

The easiness of copying information and storing them in backups renders the permanent erasure and its insurance almost impossible.

The Right to be forgotten is a valuable tool that can help and improve the lives of individuals. For example, enabling this Right can unburden the weight of previous criminal convictions, which is usually seen as a red flag in interviews and help them change their life for the better. Moreover, people who have experienced severe illnesses like cancer can enforce this Right and, after some years, subscribe to health insurance without facing warranty exclusions or paying extra premiums.\textsuperscript{53} So it is a valuable tool to battle inequalities and loss of chances due to previous diseases or former mistakes.

\subsection*{2.7 Right to Access}

The Right to Access allows smartphone users to demand transparency and gain control over the data that have been collected by their smartphone applications. The EU data protection laws give consumers the Right to access the data that companies hold about them. However, many data controllers fail to meet their requirements and refuse to provide data to data subjects. There is a general lack of responsiveness combined with incomprehensible language and malfunctioning links which has even produced data leakage. In addition,
many app vendors did not respond adequately or tried to respond in a misleading or deceptive way. Moreover, there are cases where personal data were dissolved due to inactive accounts without noticing the user. It is of high importance to develop a standardized process for subject access with standard interfaces and better support for data controllers in order to comply and implement the best practices.  

2.8 DPIA
According to article 35(1) of the GDPR performing a DPIA is obligatory for controllers when a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons. DPIAs are a set of processes that are used to identify the risks related to a data protection project and minimize them. Mobile applications have access and process personal data, which can result in a risk for the users; thus, DPIA is mandatory for app providers. A Data Protection Impact Assessment is performed in three stages, Preparation, Evaluation, and Reporting.

During the preparation step, the following are conducted:

- the obligation to carry out a DPIA is considered in correlation with the case.
- The goals of the assessment are pointed, and it is verified that the DPO has sufficient resources.
- A standard model is used to ensure transparency.
- The target of evaluation is set.
- Identification of the Actors involved and affected.
- Identification of other relevant legal requirements like national legislation.
- Documentation of the whole stage.

During the evaluation step, there is:

- An identification of protection goals.
- Identification of potential threats and attackers and their motives objectives.

---

• Evaluation criteria and benchmark.
• Risk evaluation takes place.

At last, during reporting and safeguarding step:

• Identification and implementation of the appropriate measures take place, and a risk management plan is created. There is also a prioritization of risks and measures to remedy them.
• Documentation and publication of the report using a standard form.
• Auditing of the report from a third party authority.
• Supervision and continuous review in order to adapt to changes.⁵⁵

**When to conduct?**

DPIA should be carried out when a process of data is about to happen, which can pose as a risk for the rights of an individual.

• When data are constantly evaluated in order to analyze the personality of a natural person using automated process or profiling and decisions which have similar consequences for those concerned.
• When sensitive data are processed on a large scale, including criminal convictions and penalties.
• When public areas are constantly being monitored.

The difference with risk management is that no residual risk exists, and every processing of personal data should be justified.

It can be regarded as a system that provides warnings and addresses potential problems during the process. It is used to prevent risks and implement data protection, helping for better decision-making during implementation and preventing potential damage from leaks. It can also reduce the cost of afterward improvements and demonstrates compliance with

---

the legal requirements. It can also help data protection authorities to find weaknesses and have a better scope on how to improve their products.\textsuperscript{56}

DPIAs are meant to improve data protection by increasing the accountability of the organization involved in risky processes. However, by conveying some of the responsibility to regulate to the industry raises the question of how adequately it will anticipate and address possible harms.\textsuperscript{57}

### 2.9 E-privacy Regulation

The new ePrivacy regulation will replace and align the e-privacy directives of EU member states of 2002 and 2007. The new e-privacy law is considered urgent since GDPR is not enough to change the surveillance model and to ensure the privacy of communications.\textsuperscript{58} It uses the definitions of privacy and data protection of the GDPR and takes steps to enhance them while at the same time keeping up with the pace IT services and technologies are evolving. The ePrivacy Directive, which was released in 2002 or as it was called the “Cookie Law” will be updated and cover areas like unsolicited marketing, Cookies, and Confidentiality. It was proposed in 2017 and was believed to take effect simultaneously as the GDPR; however, the final text is not agreed yet and is still being discussed in the Council of the European Union. The most important aspects will be the following:

- Cookies will require specific measures for different forms of usage, and stricter cookie policies will be applied; for example, the use of cookies will require consent except if the cookies are necessary for transmitting data. This means marketing cookies could be opted out. Furthermore, users will be able to refuse the use of certain cookies, and the withdrawal of their consent should be made easier.


Moreover, consumers should be able to have access to every service even if they refuse to cookies.

- Direct marketing will also require consent unless there is an existing business relationship, and like the cookies, customers will have the opt-out option. Furthermore, it also addresses unsolicited communications and prohibits the use of automated calling systems without human intervention.

- Control and confidentiality of electronic communications. Customers will have the Right to block numbers and be excluded from public directories. Additionally, electric communications in the form of data, metadata, and voice recordings will be treated as confidential and will require consent in order to be disclosed. This also applies to IoT communications and public Wifi networks. Interception of communications and storage of electronic communications without consent and previous notice on the user shall be prohibited.

- Storage and erasure. Metadata and communication content should be made anonymous or deleted by service providers.\(^{59}\)

- Consent\(^ {60}\) there will be stricter consent requirements, like companies reminding their customers twice a year of their Right to withdraw their consent, and consent should be easier to withdraw every time the user wants.

All the above will have an efficient enforcement across the EU member states just like the GDPR, and any violation will be fined up to 4% of the worldwide revenue.

**How will it affect mobile apps?**

Services like WhatsApp, Facebook Messenger, Viber, which are used for sending messages or online video calls, will fall under the scope of ePrivacy regulation. Until now, rules about privacy covered only the traditional telecommunication providers, but


now all electronic communications like the above will be regarded as confidential and will apply to internet-based communication services. Furthermore, it will guarantee privacy for the content of communication as well as the metadata like location and duration of calls. The kind of data will be deleted or anonymized only with the customers' consent.

With the ePrivacy Regulation, confidentiality of machine-to-machine communication is protected. This will affect Wifi and Bluetooth signals which are used by smartphones. In order to establish a connection via Wifi, a device constantly broadcasts its MAC address, and this information may be used to reveal the location of a user. Since location data is really sensitive, modification may be needed in the way communication between devices is happening.\textsuperscript{61}

Consent is aimed to be more user-friendly and with the ability to opt-out, and cookies will be used only for necessary tasks. Moreover, information about the data usage of each cookie will be required before consent is given. The above will change the way advertisements on applications works and how installation and usage of the application will function. It is also high possibly to affect the permissions security model that is used by smartphone operating systems.

\textsuperscript{61} G. Gonzalez, P. de Hert, & V. Papakonstantinou. (2020). The proposed ePrivacy regulation: The commission's and the parliament's drafts at a crossroads? In D. Hallinan, R. Leenes, S. Gutwirth, & P. De Hert (Eds.), Data protection and privacy: Data protection and democracy (pp. 267-298). Hart Publishers
3. Smartphone Ecosystem and actors involved

This chapter introduces an application’s ecosystem from the development phase to end-users utilization of the product. Further, people involved in the smartphone ecosystem and their roles are also presented. There is key terminology behind mobile application software and hardware. All actors and relevant processes addressing privacy and data protection compliance are highlighted.

The time we used mobile phones only for voice communication is long gone, and with the rise of smartphone applications, mobile phones have evolved into computing platforms. With the use of faster internet (cellular, Wifi), users have started to prefer smartphones and tablets instead of traditional computers, especially for tasks like social media, news, banking, and applications. All this technology and provided services are based on the smartphone ecosystem described below.

3.1 Smartphone Ecosystem

A smartphone ecosystem is compromised by the hardware and software platforms with many vital elements. Users are the final consumers of what applications offer. The OS and the sensors are mechanisms that can acquire permissions and personal information. Applications are the primary source of services that are used by the users and have access to data types. Developers are the ones who develop and share applications through app stores. App stores are the sources of the applications used and communicate with both the developers and the users. There are also other entities like operators, manufacturers, third-party advertisers, and more.

The smartphone ecosystem embodies hardware, software including applications, the application markets. The key elements in any given smartphone ecosystems are comprised of:

Smartphones that are devices equipped with state of the art sensors and provide service capabilities to users.
Developers are the individuals who design and develop an application for devices and share them through app stores.

### 3.2 Apps
Applications are the primary way of delivering a service to users from their smartphones. To successfully deliver a service, they need to acquire access to an individual's smartphone's data types, sensors, and permissions. There are three types of Apps offered

1. **Native**
   Native applications are designed for a specific platform like Android or iOS and can use all the device's capabilities like the sensors. These apps are found and downloaded by an app store and can operate more quickly due to their native design.

2. **Hybrid**
   Hybrid applications can also be installed on smartphones just like the native ones, but they operate on web servers, so they are slower and less reliable than native. Most of them allow cross-platform development.

3. **Web Apps**
   Web applications are written on HTML5 and can be accessed by a web browser; thus, they can operate outside the app stores. They have the advantages that they don't take up memory or other resources of the device, but they need Internet access for most of their services.

### 3.3 Permissions
Permissions is a system firstly adopted by Android in order to improve security and provide the users with the ability to choose when or for how long an application will have access to specific data. Permissions have different types depending on the scope of use. By default, most applications have limited rights, but additional permission is required whenever an application needs to gain access to sensitive data or services. Permissions are included in the application's Manifest as simple text.\(^62\).
Install-time permissions

Install time permissions provide limited access to restricted data which has a minimal impact on the system or on other applications. When a user installs the application, the system automatically grants the permissions required and provides the user with a notice of what access may the given application have.

Normal permissions are permissions that provide access to data and actions but present little risk, so the system has an average protection level for these permissions.

Signature level permissions require the same signing key in order to efficiently communicate with another application.

Runtime permissions

Runtime permissions are also known as dangerous permissions because they give the app access to restricted data and allow it to perform actions that can have a high impact on the system and other apps. Whenever such permissions are requested, the user is being asked if the app is allowed to access the specific data. Sensitive data like location or microphone access are sensitive information; therefore, the system has to explain why the app requires access to this information. Furthermore, the system assigns the dangerous protection level to runtime permissions.63

Special permissions

Special permissions are defined by the manufacturer and are used when protection to powerful actions is needed.

The permission architecture is used to protect user data and sensors. When granting access to resources can have a severe impact on the personal information stored on the smartphone.

63 https://developer.android.com/guide/topics/permissions/overview
Permissions can be used and as security mechanisms. The required permissions of an application could work as a warning for the user. An automation tool used to identify applications in the same category that require additional or different permissions can help provide a warning about malware or privacy risks. Additionally, it can be used to provide recommendations regarding privacy by identifying the permission request patterns.\(^{64}\)

When a user tries to install an application from an online marketplace, is being asked to grant a set of permissions for the app to access or use some of the mobile phone's features and information. However, most of the time, users just ignore the warning messages without understanding the true meaning of given permissions. This is possible because the users not only don't understand clearly the terms and words but also because these warning signs are shown after the installation of the app where the user just wants to continue to the use of the application without being interrupted.\(^{65}\)

For example, a user needs to make a decision about granting permissions in an application before installing it and using it so he can evaluate the benefits of having or not having this application. Furthermore, these interfaces don't inform the users of the frequency, destination, and purpose of the data sharing, so users can't even compare applications with their counterparts. Most application users were not aware and for sure not comfortable about the amount of data that is being shared by their applications, and this is troubling because the advertisement and application industry maybe working on the assumption that every consumer understands the exchange that is taking place between free application and data sharing.\(^{66}\)


IOS and Android have started to offer their users some kind of control over the permissions for each app, letting them, for instance, to toggle them on or off depending on the task. But with each application needing at least three permissions and taking into account the average's user's preferences and the quantity of the installed apps, we can understand that it is highly unrealistic for a user to configure and control all these permissions having privacy and the protection of the sensible information in his mind.67

How many permissions a user gives to an application depends on the age, the education level, their preferences, and if the application is free or paid. Paid apps tend to ask for fewer permissions. Another thing that influences a user's choice to grant or not some permissions to an app is based on whether the request is needed by the app to be functional or it is used to share information with an advertisement company.68

Disabling permissions can affect the usability of applications. In some cases disabling permissions for a specific application can have an impact on the way an application work. It is easy to assume that removing the camera permission from the flashlight app will render it useless, but it is crucial to understand why some other permissions not connected to the main functionality of an app can influence the way an application functions. Change on the combinations of permissions can have different results on usability.69

3.4 Operating system providers
Nowadays, in the smartphone environment exist several operating systems like Tizen, Windows Mobile, EMUI for Huawei, but the two most prevailing are Google's Android and Apple's iOS. They are more operating systems designed by different companies but either discontinued or declared obsolete. Android is an open-source project launched by Android


and later acquired by Google. It uses a customized Linux kernel and accommodates applications that are isolated in their own sandboxes, using permissions to access other services. iOS was introduced by Apple, and it is developed exclusively for its hardware. It uses a kernel called XNU, and it also sandboxes the application allowing them to modify data only into their directory while using a permission model to provide access to additional services.

3.5 Users
Users are the endpoint of the smartphone ecosystem. They are the consumers who utilize the services and applications provided by the app developers. Users spend a majority of their time using smartphones, and most of this time is spent connected to the internet and utilizing an application. Around 90% of a user's time is spent on mobile applications for enjoyment, social interaction, online shopping, education, fitness, and many other application categories. The smartphone users are expected to grow to 5.5 billion by 2022\(^{70}\) showing a growth beyond expectations with expected revenue from mobile apps to reach more than 935.2 billion dollars\(^{71}\).

3.6 Network Communications
In order to connect to the internet, every application uses either HTTP or HTTPS protocols to connect with services back-end. In order to be able to use the internet, access permission must be accepted. HTTPS is the preferred protocol because it is more secure, and mobile devices use many public hotspots that are less secure. Application communication with the servers is also required. Transport layer Security (former SSL) can provide encrypted communication between clients and servers by utilizing public-key cryptography. GDPR states that appropriate security measures for secure data transfer should be taken.

---


3.7 Unique Identifiers
In order to identify a mobile device, a hardware identifier called the International Mobile Equipment Identity (IMEI) is used and provides a unique number that cannot be tampered with, and it is different for every mobile device. The same is valid for MAC addresses that are used by the radio signals (Wifi, Bluetooth).

3.8 Storage
The most common concern regarding security for Android applications is how secure are the data stored in internal or external storage and if these data are accessible by other applications. By default, Android provides sufficient protection for most applications by limiting access to data only to the specific application. In order to provide additional protection, especially for sensitive data, encryption is highly recommended. Furthermore, if there is a need for data sharing between applications, a content provider can be used which offers dynamic permissions depending on every case.
Due to its transferable nature, external storage is more vulnerable than internal storage. Encryption on external storage is highly recommended as much as the avoidance of storing sensitive information or executables on the external storage.

3.9 Application stores
Applications stores play a critical role in the distribution of the applications and have a significant role in the evolution and in the great expansion of applications. Application stores provide a service for users to browse and download applications for mobile phones, tablets, or even personal computers. The most successful and best-known application stores are the Apples App Store and Google Play. In this environment, developers provide their products, and users consume them. There are also many other application stores, especially in China, where the Google Play Store is not available, and since China has one of the largest smartphone users, more than 800 million, the market is distributed to domestic shareholders. For the 1st quarter of 2021, Google Play offers 3,482,452 applications and Apple App Store 2,226,823, followed by Windows Store and Amazon Appstore.72 By providing developers a market to sell their application, and payment handling led to a

massive entry of many small and medium software firms as also as individual developers. Application stores provide an online marketplace where app developers and potential customers can interact with each other and process the payment. They also offer statistics, reviews and act as middlemen who generate significant revenues from the transactions and the subscriptions.

3.10 Mobile App Developers

App development can be accomplished almost by anyone with some coding skills. However, there are also apps that are developed by entire teams and multinational companies having a lot of support and legal teams. Since millions of users can use applications, high security and privacy requirements are of utmost importance. Data compliance for someone tinkering alone an app may differ from a larger company with higher expertise. The latter has the knowledge, time, and money to implement data protection recommendations. Developers have the most significant impact on user privacy if they make different design decisions regarding personal data use. Current technology could not provide enough capabilities to audit and detect all privacy issues of an application relying on how much the developers are willing to comply with privacy requirements. Studies show that this is still really challenging for developers since there is a considerable mismatch between the actual privacy risks and the perceived risk by developers.

While there is a general awareness of the need for security measures, there is also a lack of understanding of data protection best practices by small companies of app developers. The three main security problems of mobile security are data confidentiality, privacy, and trust. Data confidentiality is considered to be one of the fundamental problems in mobile devices.

Analysis of apps has shown that developers who offer free or low-cost applications are more likely to request more privacy-sensitive permissions. So it is easy to understand that private information in mobile applications can be considered a means of payment.

---


highlighting money for privacy trade-offs used in the market. On this ground, privacy can be viewed as something that can be negotiated between the consumers and companies if the consumer is given the right to manage his own data.\textsuperscript{75}

Application developers use their skills in order to write software for mobile devices, depending on operating system they are working and upgraded their skills based on the system they are working on. The most common types of application developers are the iOS and Android.

The design and the way an application functions depend not solely on the developer and his methods but on the entire mobile application ecosystem. This ecosystem consists of hardware, software, operating systems and protocols, and many more. So even the influence of an app developer can be limited, and there is a need for a holistic approach in protecting privacy. This complexity puts obstacles on developers who, even if they are aware and trying to comply with the legal requirements, face struggles due to limitations of the other members of the ecosystem, as mentioned earlier, such as the OS providers.

4. Compliance and Data Protection Challenges

In this chapter, we discuss and present the most common compliance and data protection challenges for mobile applications. We analyze the reasons that are responsible for the emerging risks. There is a discussion about hardware, software, and even the human factor and the role all the above play in data protection.

Mobile applications are now quite perceptive about personal information by constantly demanding additional access to sensitive information in order to provide a more personalized user experience. That kind of privacy-invading practice has caused privacy concerns amongst app users.

Applications installed by a user can reveal a lot about user behavior, interests, and habits. Using machine learning techniques and installed applications on a user’s smartphone could lead to recognizing various personality traits of a user automatically. Furthermore, any four apps installed by a user can be used to re-identify a specific user from a dataset. This points out that there is a great need for better protection of collecting, using, or sharing the list of installed applications that were really easy to obtain. It is really important to recognize specific compliance and data protection challenges in order to be able to mitigate them and inform all the actors involved how to be more data protection aware.

4.1 Cross border Transfers

Nowadays, digital systems have services worldwide, and data flows to different countries. This can be a substantial potential risk to privacy since the communication of personal data in different countries is subject to various data protection laws with different levels of protection. Mobile applications collect a tremendous amount of personal data, which are then shared with data processors or third-party services. Application stores are global, thus

---

making apps available for users in their country of residence. GDPR offers protection to application users in the EU and even protects their data outside the union. It also includes specific criteria in order to allow the cross-border transfer of data.

Almost ¾ of the applications tested transferred some personal data outside the EU. More than half of the analyzed applications are potentially non-compliant with the cross-border requirements of the GDPR, revealing a gap between what is done in practice and what GDPR regulates. Application providers lack transparency from third-party services like libraries embedded in the code and may be responsible for the cross-border transfers. Although app developers are expected to understand and know how these libraries work and share data, evidence indicates that this is not the case. Furthermore, these third-party libraries usually do not provide a privacy policy and do not share information about their practices. Moreover, explicit consent could be used to enable cross-border transfers if it is obtained as it should. However, in most cases, app providers state that downloading and using the application by a data subject is an implication of consent, so there are no additional measures needed.77

Users should also be informed about the app provider's security measures if their data is processed outside the EU.78

4.2 Risk data practices of Developers
There are data practices used by developers to achieve certain features for their application and can result in risk without the developers perceiving them. Some of the risks identified during a case study on a developer forum are the following:

- Sending data out of the device
- Sharing data with third-party libraries and services
- Storing data on remote servers
- Storing data on the device
- Sharing data with other users

---


78 (Art. 13 (1f), Art. 14 (1f), GDPR)
Collecting data in the background

Sending and storing data outside of the device or on remote servers increases the possibility for data leakage due to security reasons or can result in secondary data usage that is permitted without the user's consent. Furthermore, sharing data with third-party libraries can lead to the misuse of data by these parties in a negative way.

Storing data on smartphones can result in a potential risk regarding the data retention period. For example, will the same apply to the data if the application is uninstalled or removed? Moreover, the storage on the devices is prone to malicious attacks and can possibly result in unintentional data leakage.

Background data collection violates the users' expectations of how their data are being used and if those legitimate purposes are met. Additionally, specific consent is required for this practice of data collection.

Sharing data of their users could produce misusage of the data for other reasons than the ones the data subject is informed and probably consented to.

While almost all mobile applications require from their users to accept the terms and conditions before launching the app, it is commonly accepted that the majority of users skip the long pages on their small screens and just accept everything. By doing so, they trust the app developer with their best interests regarding their data in mind. Except reading the terms and conditions, a consumer can do almost nothing; even if the consumer can understand the potential risks and denies the terms, he/she immediately loses the capacity to use the application. On the other side, there are ample decisions a developer can make that can improve the privacy and the protection of a consumer.

Many developers think that compliance with the app store is sufficient and that the app store is responsible for legal protection or for monitoring them if they meet the compliance criteria.  

---

It is still common that application developers collect data on the basis of broadly construed general purpose, which is not sufficient to comply with the GDPR’s obligations. So for instance, processing personal data “to provide the service and develop new features and future services” is too general to be able to comply with the legal requirement of purpose specification.

A transparent and easy-accessible privacy policy about personal data is one of the most critical requirements for organizations in order to be GDPR compliant. However, still many mobile app developers do not provide complete privacy policies, or the ones provided are outdated. For example, the user's active and informed consent is needed before any personal data can be collected. However, many apps assume that a user’s decision to download and install the app is equivalent to consent for the collection of their data. Furthermore, many policies have vague descriptions about the usage of information or intentional ignorance by the developers who believe some kind of data is not essential and proceed to collect them without informing their users. In other cases, even if confidentiality is highly appraised and reasonable measures are declared to be implemented in order to secure the data, there are many app developers who need to enhance their data protection methods and at least provide the standard security measures.\(^{80}\)

Application developers are humans, and thus they make mistakes like the users. However, when users make mistakes endanger themselves in contrary to developers who endanger millions of users and those who rely on their work. Furthermore, it is pretty challenging to identify, fix and even defend against developer mistakes. It is safe to assume that developers could benefit from additional aid in many areas, like safer programming languages, security libraries, and better testing tools.\(^{81}\)

The design and the way application functions depend not solely on the developer and his methods but also on the entire mobile application ecosystem. This ecosystem consists of hardware, software, operating systems and protocols, and many more. So even the


influence of an app developer can be limited, and there is a need for a holistic approach in protecting privacy. This complexity puts obstacles on developers who, even if they are aware and trying to comply with the legal requirements, face struggles due to limitations of the other members of the ecosystem, as mentioned earlier, such as the OS providers. Furthermore, the legal regulations focus more on providing guidance on what the developers should comply with the legal requirements. However, there are no recommendations on how to embed them in their application. But even if developers are presented with guidelines for following best practices and privacy security during all development phases from the inception of the idea until the application usage, the results reveal that there are significant differences between what is promised by the developers in the policy texts and what it is really happening in reality.  

4.3 Application Stores
While app stores provide users with ample choices for new applications and the ability to search for applications suitable to their needs, they are also a source of different kinds of malware disguised as typical applications.

Application stores are the most used platforms to sell and download applications. Apple App Store and Googles play store are the dominant entities in the distribution of applications and have enough power to apply and enforce data privacy requirements to all app developers who want to take advantage of their online marketplace and the ample users it offers. Furthermore, they act as intermediaries who process the payments between users and developers. Since trust in the online world is limited, app stores help to create a more trusting and open-to social interactions place. With the help of the customer, ratings allow both parties to communicate and improve their services or experience.

Application stores can influence the development and the security of apps by putting standards for technical and policy. App stores have specific requirements in order to publish and maintain an application on their market. Technical requirements like the need

---

for cryptographic transmission of sensitive data or specific developer policies can be enforced by rejecting apps that do not meet the request criteria. It is safe to assume that app stores can ensure a level of quality and protection for their users and influence the conduct of app developers.

In the case of AccuWeather, the applications took control of the iOS core location API in order to determine the users location, even in cases where the permission to access the specific API was denied. In that cases the application bypassed the permissions and used an interface of the iOS core where applications could access data independently of what choice a user has made.

In another case Apple is alleged using privacy protection of users as a reason for uncompetitive conduct. Specific app developers claim that their applications where targeted and removed from the iOS store, not for privacy relating concerns as Apple stated but because their applications was hurting Apple’s business. Moreover, application platforms like Apple and Google even if they set and control technical and security standards for applications on their stores, rarely publish information about removal of applications and application developers. Since these platforms play a major role on the distribution of the apps and how compliant application can be it is critically important to disclose information about the technical standards they set, the terms of service and the agreements regarding privacy to be documented and accessible and the enforcement of privacy rules for access and removal of applications should be also disclosed and published in an easily-accessible format.

4.4 Contact tracing apps during the Covid-19.
Due to coronavirus, a new challenge for health authorities and app developers appeared. The need to identify and isolate infected individuals and their contacts in order to break the infection chain and stop the spreading of the pandemic. The use of contact apps on mobile

---

phones using Bluetooth or GPS identifiers assisted in increasing the tracing accuracy but not without a cost. Current apps designs are based on two models a decentralized and a centralized one. A back-end server system was used for the centralized one to assign an identifier to every mobile app. Each smartphone broadcast using Bluetooth its identifier to nearby smartphones. The problem is that the server is in a position where an association from all the identifiers is possible and could assist in the monitoring of all the users of the system. The back-end system does not have any information about the users on the decentralized model, so it is impossible to identify them. Nevertheless, in this case, and especially in the GAP application, infected individuals are the ones that have to publish their proximity identifiers, and this would create their information public which can lead to other users being able to track the movements by profiling them and even deanonymize the data.\textsuperscript{86} The above could be considered as privacy violations since the privacy of persons is published or used by attackers while at the same time reducing the trust in the application resulting in fewer users using and publishing their data which will lead to diminishing the effectiveness of the app.\textsuperscript{87}

4.5 Transparency

Although transparency is considered critical and obliged by the GDPR, in many cases, transparency on mobile applications about data collection and sharing behaviors is elusive. Chapter 3 of the GDPR is dedicated to the rights of data subjects, highlighting its importance. Data collection and the purpose of the process should be known, who is legally responsible and how to contact that person. The app provider should also inform the users before the installation of the application and, in case of a data breach to inform its users. All the above information should be available and accessible within the interface of the application. By taking control of transparency, users will be able to consider how the usage of an application would expose their data to third parties and thus make more concerning


choices and have a better role in protecting their rights.\footnote{M. Van Kleek, I. Liccardi, R. Binns, J. Zhao, D. J. Weitzner, and N. Shadbolt, “Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps,” in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver Colorado USA, May 2017, pp. 5208–5220. doi: 10.1145/3025453.3025556.} Even though in many privacy policies, there are declarations for collecting other information relevant to users, most of the actors involved are not specified, and this vague description violates the transparency of the users.

4.6 Right to portability
Many applications do not provide users with a choice to receive their personal data in a machine-readable format. However, this right is registered through GDPR and is mandatory for all applications. Furthermore, some apps have this functionality only on paid versions.\footnote{A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, “Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice,” IEEE Access, vol. 6, pp. 9390–9403, 2018, doi: 10.1109/ACCESS.2018.2799522.} In other cases, even if the functionality was available, the way the data was communicated was either tricky or could even pose as a privacy risk.\footnote{J. L. Kröger, J. Lindemann, and D. Herrmann, “How do app vendors respond to subject access requests? A longitudinal privacy study on iOS and Android Apps,” in Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event Ireland, Aug. 2020, pp. 1–10. doi: 10.1145/3407023.3407057.} In some cases, unauthorized third parties could quickly obtain personal data by fake subject access requests. That was possible because app vendors did not ask for identity verification.

There are also disruptive or misleading responses stating that no data were collected or the accounts no longer exist.\footnote{M. Van Kleek, I. Liccardi, R. Binns, J. Zhao, D. J. Weitzner, and N. Shadbolt, “Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps,” in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver Colorado USA, May 2017, pp. 5208–5220. doi: 10.1145/3025453.3025556.}

4.7 Profiling
Article 4 of the GDPR refers to profiling as a fully or partially automated process of personal data in order to evaluate the personal aspects of a natural person. Many applications that use target advertisement fall into this category since it requires data processing of an individual’s demographic and behavior scope to determine the prospect of buying a specific product.
4.8 Rights and obligations regarding children
Children that are below 16 years old and using applications fall under a different data protection policy. The consent of their parents is required, but it is really tricky on how to ensure that all applicable measures are taken in order to verify that a parent is actually the one consenting. The design of a children-friendly digital environment can be pretty demanding and have tools that limit access to networks like social networks or even advertising that are not children-friendly. Furthermore, in-app payments and purchases should have an option to be deactivated and parent control software to be available. Moreover, in some cases. Application developers stated that they do not collect data of minors knowingly and that their applications are compliant. There is an example of a lawsuit against Disney claiming that children's data was illegally collected in 42 of their applications. In many children's applications, location data, email addresses are transmitted without user consent. Third-party SDKs are prohibited from being used in children's apps due to deceptive collection of data; the use of such libraries is still common.

4.9 Embedded sensors on mobile devices.
Smartphones are equipped with a lot of sensors like motion, gyroscope, and accelerometer. Motion sensors can be used for applying different kinds of attacks in order to reveal a user's PIN or unlock pattern. For example, locations on the screen of a smartphone can be identified by readings of the motion sensors; tapping and swiping gestures can result in patterns that are recognizable and reveal the input of a user. Even light sensors could be

92 https://www.engadget.com/2017-08-09-disney-illegally-collected-data-kids-apps.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlIlJmNvbS8&guce_referrer_sig=AAAN7OKFspZ2sApdWmN5XVD1qXA5ZaxkXVdIklns8cPcsWx8Q3UL5iPdy3PXzmlLHnyUQ8O38-QLMNaVJwb_k_8IuaeF7sgUcYTei9MTTitiVIdlScZRdi35rBHwR3_uqjm56WinxCkp_8WFuCmLz6MX9XF3MCr-PZxG-lxeMz
used in order to understand different patterns from a user tapping and be exploited to reveal Pins and input information. For all this to be feasible, a malware application needs to be running in the background that takes advantage of the sensors' readings and logs. And here lies a vital vulnerability because accessing those logs does not require any specific system permission. This demonstrates that even non-critical permissions can result in privacy violations, so system manufacturers should apply stricter security measures.

4.10 Third-party sharing
Most applications need to transfer data and communicate either with remote servers or with other applications. Since there is purpose limitation and data minimization aspect in the GDPR, it is crucial the transmission of data to in accordance with the purpose. For this to happen, data sharing should be isolated and restricted. Information like location should be minimized, and most important of all, only the data that are required for the functionality of the application should be collected and processed. Even then, a robust cryptographic protocol is needed. Furthermore new malware attacks abusing the communication between applications take advantage of the privileges each application has and then combine and use their combined privileges in order to achieve malicious tasks that are a threat to privacy and system’s integrity. For example one application have access to sensitive information but it does not require access to network so it can trick the users and permissions systems. However, another application from the same developer has access to the network but not to sensitive information. In this case the first application sends the sensitive information into the second application which then leak all this data using network access.

4.11 Third-party content
It is common knowledge that developers use a portion of code they find online and implement third-party libraries. It is highly possible that kinds of components to result in

---

accidental or intentional data leakage with privacy and security implications. It is of the utmost importance that these third-party components to be checked and authenticated before being imported into an application. Security updates and audits would be essential to mitigate risks that may arise. The ability to change the architecture of the app and remove this component in a case of violation of misbehavior would be critical to provide transparency and lawful processing of data.

4.12 Data retention
The data retention period should be clearly stated and personal data deleted after the expiration date. Moreover, confidential data like passwords, credit cards must be deleted from all storage, including remote ones, upon the uninstalation or deletion of the application, for example, in the UBER case. Uber engineers used a technique called fingerprinting, which leaves a small piece of code on the smartphone even if the application is deleted. The problem is with this technique; the developer could know if the application was installed previously on the same smartphone since many track drivers were deleting and reinstalling the application to achieve higher rankings and avoid bad reviews. Furthermore, the company was able to track users who had deleted the application resulting in a violation of the data retention period.

4.13 Privacy policies
There are cases where app developers have never read their own privacy policies, and they only use them as a necessity to protect them against lawsuits or fines. Furthermore, some developers expressed feelings that full disclosure may scare users away and avoid using their application. Regarding how the policy was drafted, some of them rely on their social friends or on online platforms and many times use default drafts. Moreover, even developers stated that they find difficulties reading privacy policies of third-party API or other services they implemented in their application.

Third-party tools could collect information about a user while having no relationship with the smartphone user and thus no real incentive to protect user privacy. On the contrary, the app developer relies on his trust and relationship with the users to promote the application, so the burden of security falls on the developer side.

App developers should claim in their policies if they are going to use sensitive information and for what specific purpose. There are policies with no basic contact information, or the statements were years old with no updates.\textsuperscript{99} An analysis of the applications and their policies can demonstrate if the above criteria are met. The need to request specific permissions from the application is usually not clarified in the privacy policy texts.

Designing a privacy policy that is GDPR compliant and easy to understand by the users could be a difficult task. Having transparency and explicit disclosure regarding personal data processing and protection is the most common compliance failure. Furthermore, failure to mention whether encryption on data exist while data are at rest and notification of the supervisory authorities in case of a breach are additional compliance failures reported.\textsuperscript{100}

Privacy policies are the best tool we have to understand how companies use our data. Even knowledgeable users have great difficulty understanding the true meaning of a policy.\textsuperscript{101} Additionally, even experts in the field disagree on the meaning of some key terms; it becomes clear that an average user will face a lot of obstacles to understanding a privacy policy. This can drive people to care less about policies and privacy threats. For example, suppose a user cares only about his credit card information and visits a site that states that it


does not collect or store credit card info. In that case, the user might feel it is ok to use it even though it is possible to use another personal data.\textsuperscript{102}

\textbf{4.14 Consent}
Consent is one of the six lawful bases for processing personal data under the GDPR. In order to be lawful, consent must be "freely given, specific, informed and unambiguous." This sentence means that an individual should make a distinct action to acknowledge consent, like clicking in a box when visiting a site. Before this action, enough information to help with the decision is required. Information about who is going to process data and for what specific purpose is essential and should also be addressed in the privacy policy. Pre-ticked boxes and any other type of default consent are not acceptable since it is not affirmative action.

Consent could be withdrawn at any time the user decides, and all the utilities it provided should be revoked.

Different kinds of consent should be used in distinct categories, like third-party sharing and children using the device. Many consent implementations offer almost no choice to consumers. It is critical for consent to be explicit and specify the exact reason and what data is going to be collected and for what purpose. Most applications fail to inform users of the exact amount of data they are collecting and for what reason. Even if they ask for consent in order to proceed to data gathering and sharing, the amount of data gathered and the actors involved in the sharing are rarely included in the consent form. Moreover, most of the time, even the app developers do not know precisely how all this data is transferred and used.

At last, consent should not act unnecessarily disruptive for the service it is provided. Furthermore, it is critical that all the services and third-party controllers involved should be named.

\textbf{4.15 Use of untrusted Content}
It is quite possible for a mobile phone to encounter untrusted content than other types of devices like personal computers. For example, Quick Response codes (QR), they are

\footnote{A. M. McDonald and L. F. Cranor, “The Cost of Reading Privacy Policies,” 2009 p. 22.}
designed and used in many shops, in cafes, and restaurants in order to access the menu, and even the COVID-19 passport utilizes such codes. QR codes are processed by the mobile phone's camera and translated into text, which is a URL link. However, with a bit of tampering, such codes can lead to malicious websites and perform different kinds of malicious attacks. In some cases, such codes do not provide the user the choice to be redirected on the website but proceed unobfuscated depriving the user of the choice to defend.

4.16 Authentication
Mobile devices and applications need the ability to identify each user and device in order to authorize access to specific data and services, or not.

Protecting both mobile devices and applications from cyber attacks is one of the most important challenges in order to ensure mobile users' security and privacy. Countermeasures should protect data, hardware, and software at all the stages.

4.17 Privacy
Smartphones are small in size, and most of the time, their worth is high; thus, they are the perfect target for thieves. It is also common for many people to lose their phones. Furthermore, a stranger can easily tamper with smartphones without locking mechanisms if they are left unattended. Someone can install spyware or simply have access to a lot of our personal data that are stored in our smartphones. Both the above examples can lead to confidentiality and integrity loss.¹⁰³

4.18 Supply chain
During the development of pre-installed software, a lot of actors are involved who have privileged access to the system by their applications or third-party libraries which are used in the development of the apps. Potential deals and partnerships between organizations can

take advantage of a user’s data before the installation of software of their liking even on new devices.\textsuperscript{104}

### 4.19 Transmission
GDPR requires developers to provide appropriate technical safeguards to ensure the security of the transmission of personal data. Although it is not explicitly stated what measures should be applied. Encryption is one of the most prominent tools for security in communications used in applications. However, even with encryption, there are studies\textsuperscript{105} that demonstrate that even weak encryption algorithms were used and sensible data were not adequately protected. Furthermore, another encryption technique resulted in insecure information due to constant algorithmic keys. During communication on the Android platform, SSL or TLS protocols are the most common, which are vulnerable to Man in the Middle Attacks. Most of the applications use SSL protocol with inadequate validation and code that accept all the certificates for validation. Insecure transmissions like the above are critical because they can expose sensitive data. Confidentiality is at stake in many applications which even though they have declared in their policy that reasonable measures for securing the data will be implemented, failed to do so. In some cases, they fail to use the suggested methods or misuse them having again negative impact.\textsuperscript{106}

### 4.20 Permissions
In order to protect sensitive data, permission model was implemented. Asking for permission to access data or services is possible to result in higher security or not?


When permission first appeared in the Android OS, users had to accept all permissions an app required in order to install it. The same was applied for new releases and updates of the applications, even if it included permissions which can be dangerous—realizing that, app developers tend to ask for more permissions since users were willing to give them. Since updates and changes on applications occurred at regular intervals, app developers used to ask for extra permissions in first releases having in mind that since users will grant them anyways, they can use the permissions in later updates without asking for additional approval. This leads to many apps being overprivileged and posing a high-security risk. After Android 6, Google changed the way permissions operate into a more dynamic one that asks for users' consent when they use permissions and has simplified the model by creating permission groups.

Systems now grant permissions automatically depending on the permission. Automatically permission granted is also used when an application has already acquired a permission from the same group. For example, if an application has permission to Receive_SMS, the system automatically grants the SEND_SMS permission to the application since they belong to the same group, but the user is not notified or asked for additional consent. This could lead to malicious users exploiting the permissions that an app already owns in order to gain access to more sensitive data. Studies show that in an android store, over 17% of the apps have requested at least once in their lifetime dangerous permission that the OS has automatically provided without the user's approval. Moreover, almost over 50% of these automatically granted permissions allow users to access sensitive data like user's location and the list of phone calls.107 These data were communicated to servers belonging to the applications developing company or to third parties.

It has been observed in different applications that declared permissions remain unused. This can be an implication that a sleeping functionality exists in the app, waiting for a chance to harvest additional data. Furthermore, it is observed that applications are asking for more

permissions that are related to Sensors even more than in the post-GDPR era. A possible explanation for that is that advertisement content is way more effective when the user is looking at the screen, so it is quite possible for applications using motion sensors and bearing to determine when is the right time to have the greatest impact on the user's interest.\textsuperscript{108}

When a user tries to install an application from an online marketplace, he or she is being asked to grant a set of permissions for the app to access or use some of the mobile phones features and information. However, most of the time, users just ignore the warning messages without understanding the true meaning of given permissions. This is possible because the users do not understand the terms and conditions. These warning signs are shown after the installation of the app, where the user just wants to continue to the use of the application without being interrupted.\textsuperscript{109}.

\section*{4.21 End-User}
The human factor plays a significant role in data protection and in privacy-preserving tactics in mobile applications. Except for the application developers, the users can change a lot in the way they use their mobile phones and the information they provide in order to improve security and privacy. The lack of user awareness is the number one reason for privacy leaks or for cybersecurity attacks that are based on social engineering like phishing.\textsuperscript{110}

Users also tend to be in a rush to install even applications that are potentially dangerous and many times share personal information without having second thoughts. Moreover, most people do not spend time reading a privacy policy and just accept everything in order to use the application. The same applies to consent. As far as the permissions are concerned, even aware users tend to give extra permissions in applications even if they know and

\begin{thebibliography}{110}
\end{thebibliography}
understand the potential risk. Another important aspect is that nowadays, an average user has more than 40 applications installed on their smartphone. Some of them do not use any security lock because they find entering patterns or passwords annoying. IOS and Android have started to offer their users some kind of control over the permissions for each app, letting them, for instance, to toggle them on or off depending on the task. Nevertheless, with each application needing at least three permissions and taking into account the average's user's preferences and the quantity of the installed apps, we can understand that it is highly unrealistic for a user to configure and control all these permissions having privacy and the protection of the sensible information in his mind.\footnote{B. Liu, J. Lin, and N. Sadeh, “Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help?,” in Proceedings of the 23rd international conference on World wide web - WWW '14, Seoul, Korea, 2014, pp. 201–212. doi: 10.1145/2566486.2568035.}

But even then, the average user does not understand privacy policies, and even experts cannot agree on the meanings of certain terms.\footnote{A. M. McDonald and L. F. Cranor, “The Cost of Reading Privacy Policies,” p. 22.} Furthermore, most people never read the policies or do so once per year. This happens because policies are too long to read them, difficult to understand, and sometimes ambiguous on key terms that result in people not being able to understand the language and what is hidden between the lines.\footnote{J. Kang, H. Kim, Y. G. Cheong, and J. H. Huh, “Visualizing Privacy Risks of Mobile Applications through a Privacy Meter,” in Information Security Practice and Experience, vol. 9065, J. Lopez and Y. Wu, Eds. Cham: Springer International Publishing, 2015, pp. 548–558. doi: 10.1007/978-3-319-17533-1_37.}

\section*{4.22 The role of users and consent. Pre-installed software}

The open-source environment of the Android OS allows smartphone manufacturers to pre-install apps which can be pretty intrusive and have tremendous implications on privacy and security.

The average Android user is unaware of most software and the applications that come pre-installed on their new smartphone. There are a lot of data-sharing relationships between companies and enterprises that are responsible for the software that exists in brand new phones. Users, of course, have never consented to acquire these applications, and most of the time, they cannot even delete them without interfering with the regular function of their phones. These applications can collect and monitor users' personal data without their
awareness, let alone their consent. Even new devices did not present a privacy policy during the first boot, and if they do and a user does not accept them, the device becomes unusable since it does not boot. The lack of a precise mechanism to obtain consent is a potential violation of the GDPR and other consumer protection laws.\textsuperscript{114}

Pre-installed services are also called "bloatware," have privileged access to system resources, and it is possible to expose critical services of the smartphone and data even if official Android permissions restrictions apply.

### 4.23 Storage

Applications store data remotely or into the internal storage of the smartphone. It is imperative to be mindful of storage limitations regarding the personal data collected. Furthermore, data leakage is a real problem that can occur due to riskware applications which require a broadside of permissions and take advantage of them in order to send data to third parties. According to OWASP's top 10 application risks, insecure data storage is the number 2 risk. Wrong encryption techniques and insecure mechanisms in storing data can result in data leaks.\textsuperscript{115}

### 4.24 IN-APP payments

Applications downloaded from application stores are either free or come with a cost that is known to the consumer before downloading. The problem arises when there are additional costs within the app and users are not aware or adequately informed. The user should be informed in a comprehensive way about the total price and taxes, and in addition, it is required for him to consent before a transaction takes place. However, in many app environments, there are build-in purchases that are being charged after the installation and gaining some extra attributes by using the default payment method, which is stored in the app store. Furthermore, for these purchases, no additional consent is required\textsuperscript{116}, and the


\textsuperscript{115} https://owasp.org/www-project-mobile-top-10/

\textsuperscript{116} Iglezakis, I., Samartzi V., Papadimitriou, R., Smyrnaki, E., 2019 The protection of users of mobile applications. Journal of internet of law, 23, (2).
user is informed that the default authentication setting is set at 30 minutes allowing purchases to be made without a password and consent.

4.25 Mobile application security threats
Mobile users are subject to malicious activity like malware applications for smartphones. Some of them are:

- phishing in applications, these apps are typical applications that can bypass the app market regulations by not having anything malicious inside their app, but when they are being used, they redirect the user to another malicious site outside of the application.
- Supply chain compromise. A malware version of a legitimate application is being included in the factory firmware and shipped on customers with new smartphones. The original applications are modified and include malicious code in order to have a different purpose, intercept and send SMS without the user knowing. This malicious version could be installed into the supply chain in many different places, and it was never available for downloading through an app store.
- Cryptominer code in some games or utilities is a malicious code inserted in several applications without notifying the user and run in the background mining cryptocurrency when at the same time uses the phone's utilities and draining its battery.
- Click-fraud advertising embedded in applications forces or redirects users to click on some advertisement, and by clicking on the ads, ads accumulate wealth making it one of the most profitable criminal enterprises.117

Whenever a user installs a new application on his/her smartphone is at the risk of installing malware; in contrast to desktop applications, mobile ones to access a lot of sensitive and personal information. A smartphone application, in order to be fully operational, has access

---

to many functionalities and sensors, but this wide access can also be harmful since it also provides the opportunity for malware to take advantage and misuse the collected data.  

4.26 Use of untrusted applications.
Mobile devices are designed to make it easy for the user to download, install and use applications for everything he desires and include applications from third-party developers. Since this can pose a major security risk, organizations need to point their security into the assumption that all third-party applications may be used by the user, but they should not be trusted. In order to reduce risk from this kind of apps in an organization's mobile device is to whitelist only approved applications, perform risk assessments for new apps, implement a sandbox that is isolated space for sensitive data, and only allow the necessary permissions. Furthermore, it is possible to access these apps through web browsers on smartphones, there are additional mitigation strategies like restricting browser access, using secure gateways or proxy servers are some of the steps that can be used to reduce risk from untrusted applications on smartphone devices.

4.27 Location-based mobile applications (LBMA)
The accelerating proliferation of smart devices has led to the expansion of mobile applications and the development of location-based services. These applications and services use satellite technologies like GPS and Glonass and are mostly smartphones and wearables (smartwatches). Location-based data are information that is collected from applications and used for multiple purposes such as transport services, availability and offers of products, and even tracking their moves for health reasons during the COVID-19 pandemic. When using such applications, users might be aware that part of their privacy is

---


119 Souppaya, M. and Scarfone, K. (2013), Guidelines for Managing the Security of Mobile Devices in the Enterprise, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-124r1
being exposed and their private information shared, but there are some cases that consumers may believe that this trade-off is probably worth it.\textsuperscript{120}

Proper handling and managing of applications is essential for mobile phones security since applications installation and managing (source of download, updates, permissions) are the main areas used for exploitation.

There are many classes of mobile attacks, but we will focus on application attacks which can be error messages, pop-ups inside applications, malicious advertisements, clicking frauds, rootkits, and Trojans.

The source of the download of an application can be considered as an indicator of risk. Applications from dubious sources are more likely to be malicious than applications from the official markets.

\textbf{4.28 Application handling}
The security concern does not end once an application has been installed. A user needs to make additional decisions regarding security while using the application. Decisions like permission granting, privacy settings, updating can also pose as security risks, and a user need to be security-aware. Information security awareness is needed, for example, when a user needs to decide whether to update an application or not. Updates are usually used for fixing bugs and covering security vulnerabilities. However, it is also possible that an update can result in changing the form of an application and render it malicious.\textsuperscript{121}

One important aspect of GDPR is that it requires software that handles personal data to be compliant not just the time it is released on the market but to ensure an ongoing compliance with the conditions of the regulation. Since building a piece of software once and never changing anything is quite rare for a piece of software, bug fixes, updates, and


improvements should also prove to be compliant with the regulation. In this way, an ongoing protection is ensured for the users and, in combination with the drastically increased amounts of penalties (up to 4% of a company's worldwide turnover), heightens the importance of efficient strategies.\textsuperscript{122}

\section*{4.29 Big Data}
Using big data analytics large amount of aggregated data can be analyzed and used because this kind of data is anonymized. Anonymized data are not considered personal data, so data protection laws do not apply to them. However, with large quantities of aggregated data, even if identification of an individual is not happening, it is possible to identify patterns and behaviors which can be used to construct some profiles and even predict decisions of an individual. In this way, anonymized data that are not protected by laws can influence privacy and even put at risk the fundamental rights of a person. Anonymized data can have a significant impact upon a person since using data points of a specific person can result in higher insurance costs, sharing of online behaviors, public transport, etc.\textsuperscript{123} The use of anonymized data is widespread in the advertisement industry. These companies are not interested in the actual identity of a consumer. However, they are really interested in his shopping habits and how likely their advertisement is to impact the average consumer. So even if the collection of anonymized data is not used for identification, we can understand that it is being used in a way that can be also be damaging to a person's privacy and independence.\textsuperscript{124} In big data environments, users' personal information is accessed through smartphones, shopping records, etc., and usually without their consent. Furthermore, the fusion of public data with private data creates risks of disclosure and the like hood of

\begin{thebibliography}{5}
\end{thebibliography}

\begin{thebibliography}{5}
\end{thebibliography}
privacy violations. For example, data are generated from social media IoT devices and other emerging technologies and applications. All the above can contain an individual's private information.

So we can easily understand that the fundamental right of non-discrimination, which is responsible for the prohibition of discrimination in many contexts like employment, healthcare, beliefs, opinions, etc., can be challenged by computational pattern recognition techniques that are being used by Big Data tools.

Another crucial issue is that Big Data functions on the premise of gathering a lot of information and then creating patterns and behavioral predictions. With data minimization and purpose binding in mind, we need to think that Big Data may generate patterns that we have not predicted and usages that we did not foresee. It is impossible to know from the beginning the outcomes of the analysis; the usage and the importance of data become apparent after the mining of the data. To summarize, we can note that by using big data analysis, we gain some inferred knowledge that it may differ from the original purpose of data collection and thus create some purpose-binding issues.

With the rise of usage of wearable devices and data shared through social media networks which can be called "volunteered" data, although users do not firmly believe that they voluntarily give away their data to others.\(^{125}\) All this kind of information gathered is not only about an individual user but also about people around him or her. So consent here cannot protect a user's data, primarily when this data is being used for different purposes of the one which was initially collected.

Today big data analysis uses hundreds of data and variables to gather information about groups of people and is used for profiling and categorizing. This information has an impact on individuals and groups who do not participate in the process and, most of the time, are unaware of this form of analysis and the outcomes it produces. By using big data, new categories are generated in society, and even if their rights are safe, as we previously stated,

the personal anonymized data are mined and used. So it is essential to take measures about the collective dimension of privacy and data protection which is different from individual rights. However, it is essential to think about the protection of information regarding a group. There are cases in which analytical data are used to help specific groups’ discrimination. For example, in some U.S local police stations used a data analysis software called PredPol.\textsuperscript{126} in order to respond and prevent more efficient to crime. Using this technology, police could allocate its resources in specific areas where it was pointed by the analysis. Nevertheless, using this technique, we are against a self-fulfilling circle because it is only logical to detect more crimes in an area where more resources are allocated and less in other areas. These can have consequences that a local community to being negatively categorized even though individuals are not directly affected.

In addition, in a big data analysis, individuals cannot object to the discriminatory use of their information. Most of the time, they are not aware that they are a part of a group of categorized; only the data gatherer has this knowledge. In this way, it becomes even more challenging to address and comply with a collective data protection policy.

For many years the data subject had little choice of how to use his data when he was trying to use a service. A tick in a consent box was the only thing he could do in order to be able to use the service or even forced to make an account and comply with the default conditions; else, he was denied the use of the specific service. A lot of scandals relating to data leaks or data misuses were made the first page changed the way people saw personal data and started demanding different models when it comes to data protection and ownership. The need for more transparent regulations was imminent.\textsuperscript{127}

Public understanding of data protection tends to gain value with the passing of the years. The idea of privacy is highly valued, and the awareness of the main points of protection and


\textsuperscript{127} T. Timan, Z. Á. Mann “Data protection in the era of artificial intelligence. Trends, existing solutions, and recommendations for privacy-preserving technologies”, October 2019. BDVA.
understanding of the regulations and laws are well accepted. However, deeper aspects are rarely understood beyond this point, and there is a disconnection between the abstract knowledge and importance of data protection frameworks and the value privacy has as a right. This leads to an undervaluation of privacy.\textsuperscript{128}

4.30 Artificial Intelligence and Smart homes.
Artificial intelligence technology is rapidly evolving and is already being used on a large scale for homes, offices, and businesses. AI is found in many smart devices that are being used in our homes and outside of them, like smart cars, smartphones, smartwatches, and more.

The use of personal data by AI is not fully understood yet and can pose a significant risk to our rights. AI requires and uses extensive databases with sensitive and protected data arising concerns regarding the ability of AI to analyze data and identify users previously considered anonymous. Being able to make autonomous decisions can lead to inadvertent interferences with human rights like the right to privacy. This technology existing in home appliances and communicating with smartphone applications could be easily breached and disclose personal information about the family and sensitive data about the children, which otherwise were confidential.

Large tech companies producing smart products and home appliances with AI like Alexa and Google Home which are always listening for a wake word and can lead to data being heard or recorded.

AI is as good as the data it has access to. The mass amounts of data available for each citizen can be excellent training for AI systems. Data like medical records, tax, physical and biometric information from facial recognition software combined with the computable power of Artificial Intelligence can result in high threats to data protection. This interconnectedness between AI and data protection will require a legal framework of how personal data will be managed and regulated by this new technology.

AI strengthens data processing in an exponential way and can deanonymize data by cross-referencing data from many sources. The above makes the distinction between personal and non-personal data obscured, requiring immediate changes to current legislation.

At last, like big data, AI has the ability to identify and predict patterns of behavior which can be used to influence opinions and decisions. Furthermore, since machines function on the basis of what humans tell them to do, human biases can be carried into AI. The ability to create classes combined with a lack of diversity in the design may promote discrimination and prejudice affecting human rights.\textsuperscript{129}

5. **Application improvement.**

In this chapter, we present ways to overcome GDPR compliance and data protection challenges. We focus on the best practices and how the human factor can play a significant role in achieving better and safer smartphone applications. We offer suggestions for application developers but also end-users and policy-makers.

The design has a great power and can be used to implement security and privacy-preserving regulations. The way an application is developed can play a significant role in how secure it is and how easily to comply with regulations and future changes in later versions. Besides the design, regulators and application markets can influence the implementation of privacy-friendly techniques and contribute into making application and their services better. At last end users and how informed are they can have an impact in the data protection and contribute into having a more safe application experience.

5.1 **Data literacy**

People tend to overuse the term personal data without understanding where the specific term applies. It is necessary to point the importance of Personal data Literacy. As it is described, "information asymmetry" points out that personal data are collected in ways we may not be able to fully understand for reasons we cannot understand and are being used in ways we may not understand \(^{130}\) (the term is also being used in economics and transactions to describe when one party has more or better information than the other). So it is critical that individuals need to be educated about their data in order to be in a position where they can make more informed choices and adopt different stances towards how their data are being stored and processed and by whom. So now, it is the right time for individuals to acquire tools and resources that can help them develop a better understanding of personal information.

---

data since they are the ones who generate all this data.\textsuperscript{131} Today’s teens were born and raised in a world the internet already existed, and many adults automatically assume that teens understand new technologies and how they work. This could be a dangerous assumption because many of these technologies require critical thinking about the mass information they provide and the ways it can be used. Most of the time, we just limit access to problematic information or sharing of information without taking the time to educate ourselves and our children about personal data.\textsuperscript{132}

There are data that people give willingly to devices, for example, social media data which can be photos, locations, texts, and many more. Personal data can be also be acquired voluntarily through activities in work and in education. Using some management system in work or while studying, users generate data that are being used to predict and improve the usage of a system.\textsuperscript{133}

There is an imperative need to educate the average user on how to recognize his/her rights and how to choose products that preserve and respect the privacy. Moreover, an educated user who knows the rights and how to enforce them has a tremendous ability to influence others and promote an application ecosystem where all the data are secure.

Even if all security and privacy-preserving measures were enforced in applications, still the user's choices can have a direct effect on their privacy. For example, most people do not even read terms and conditions and privacy policies before using an application, but when they accept these terms, which are contained in writing, they are bound to a contract even if


\textsuperscript{132} Boyd, Danah, 1977-. (2014). It is complicated : the social lives of networked teens. New Haven :Yale University Press,

they have not read or do not understand the terms. People need to realize that they are still bound by the terms regardless of whether they have read them.\textsuperscript{134}

The more concerned about privacy and security a user is, the more sensitive they will be using services that might make them vulnerable.\textsuperscript{135} Users should check the default settings regarding privacy and decide if these settings address their needs. Having passwords and multi-factor authentication can improve the security of their mobile phones and, in extension, their sensitive data.

Reviewing the permissions of each application they use is quite important. Permissions play a major role in what information applications can access; understanding how permissions work and how to customize permissions for each app can drastically improve data protection. Users must understand what their personal data and sensitive information an application can collect and process are. This knowledge and the understanding that their data have significant value or the implications a possible leak can have will result in a better comprehension of data protection risks. Social engineering can be avoided if users' perception is improved and more security measures are being taken. Avoiding public Wifi networks because usually they transmit sensitive data without encryption and are prone to man in the middle attacks. Disable digital assistances or have the wake-up function off to avoid having smart devices always listening to your conversations. Use alternative search engines disk and cloud encryption remote wipe. Are some proposals that even non-tech savvy people can implement that can increase dramatically their data protection.

End-users need to understand the meaning of privacy and personal data. It is also essential to become tech-literate and be in a position where they can understand the threats and risks smartphones and their application can pose to their privacy. Furthermore, they should be more aware and try to implement only privacy-preserving strategies and technologies and, in this way, contribute to pressuring organizations to produce safer and more reliable

services and products. Lastly, by having privacy awareness, they will be in a position to evaluate the risk and make a more informed choice about using a product or a service.

5.2 Privacy policies
In order for an application to be GDPR compliant is mandatory to have a privacy policy. Privacy policies are an essential measure and a way to communicate and inform the clients how their data are being used. They should be transparent and easy to access, free of charge, and written in clear and plain language. It is of high importance that the following information is included.136:

- Identity and contact details of the Data Protection Officer, who is the representative of the organization
- The purpose of the processing of personal data and the legal basis for it
- The details regarding the transfer to a third country and what safety measures are being taken
- The retention period
- The specific rights of the data subject
- The right to withdraw consent
- The existence or not of an automated decision-making system and information about it if there is one.
- The categories of personal data obtained.
- In what form the data are collected
- How a user can delete data from the application

It is critical to specify the purposes of processing and obtaining personal data in a transparent way. The use of phrases like "for the development of new services, for research purposes," is not sufficient and must be avoided.

---

Even if an application is compliant with the GDPR or other data protection laws, it does not necessarily mean that it is also holistically secure, and additional measures should be taken regarding the protection. NIST provides a framework with recommendations and best practices that help secure applications. Security should be implemented even before the design and the coding of an application. During coding, vulnerabilities should be tested and implement security by design.

Using MARS, an automation tool that analyzes users' privacy perceptions of application by the reviews, it is proven that reviews can be a valuable source regarding the privacy of an application and can be used to address potential threats while on the same time help and inform the developers about privacy issues. In addition, it promotes the comparison in terms of privacy aspects between the same categories of applications helping users decide if an application is considered secured.\footnote{Majid Hatamian, Jetzabel Serna, Kai Rannenberg, Revealing the Unrevealed: Mining Smartphone Users Privacy Perception on App Markets, Computers & Security (2019), doi: https://doi.org/10.1016/j.cose.2019.02.010}

In order to mitigate inconsistent data collection, it is essential that application developers list all the data the application collects. After that, it is possible to specify which of the collected data are necessary for the application to function and address them in their privacy policy. This helps the users have a clear understanding of which of their data is being collected and how they are being processed in the app.\footnote{M. Fan \textit{et al.}, "An Empirical Evaluation of GDPR Compliance Violations in Android mHealth Apps," 2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE), 2020, pp. 253-264, doi: 10.1109/ISSRE5003.2020.00032.}

A privacy policy should be available in the application even if the device is offline and with no internet connection since, all applications should have the privacy policy available at regardless of the device is offline.

In order for an application to be transparent, the developer must ensure that personal data is processed only in a transparent manner that the data subject can understand. To achieve it, all data processed should be identified, categorized, and demonstrated. Even before using
the application, a list of all data that would be possibly collected should be made in order to help the developer understand what data are being processed but at the same time provide the user with transparency and access. Furthermore, all of this information should and must be included in the application's privacy policy.

In the privacy policy, there is a declaration on what and how data are being processed. To ensure purpose limitation, the services used by the application should declare which data are used and use them only if it is necessary. This will help the developer to understand what services and permissions an application can access. If the above requirements are fulfilled, the application developer would know if legitimate processing purposes exist and are being described in the privacy policy. Moreover, all stored data will have a purpose attribute and could be easily stored for a specific purpose, possibly in an isolated and protected storage.

Information about the person responsible for data collection and contact details of the DPO, purposes of the collection of data and their legal bases, third-country transfers, duration of storage use of profiling, and if the privacy policy is easy to be found at any time. Since a data subject has the right to access and request for information regarding their data, measures to satisfy this right should be taken. The ability to answer this request in written or electronic form after the verification of the data subject. Furthermore, the application should provide a way to obtain the requested information and include mechanisms that can help the data subject's authentication.139

**Data retention**

A retention policy should be also mentioned in the privacy policy, informing the users how long their data will be kept. It is crucial for personal data to be kept only for the necessary time and for the initial purpose the consent was given. After that, data should be erased, and the user should be notified. Furthermore, a user should be able to check that their data have been deleted and are no longer stored and accessed.

5.3 Consent
There are six lawful bases to process personal data consent, contract, legal obligation, vital interest, public interest, legitimate interests. For an application to use and process data, an active, informed consent is required from the user. Application developers need to inform the users about the purpose of the collection of data and offer an opt-out choice. The clarification of what kind of personal data will be collected, where it is going to be transferred, where the data will be stored, and for how long is necessary in order to provide a piece of transparent and adequate information to users. Furthermore, in order to ensure data minimization, only the required data should be collected and used. Moreover, it is required from developers to maintain a record of a user's consent for the process of data and be able to demonstrate it if it is requested. Consent should be asked for specific reasons, and additional consent should be required if different aspects are required. For example, consent for the process of personal data is required, and if a user wants to complete an in-app payment, then additional consent is mandatory.

The consent form must clearly specify how the data are going to be used and specify the exact purpose and the extent of access. The application should only collect the information that is required for its standard functionality. Data should not be stored in publicly accessible places or in an unencrypted format in external storage, data logs, or in other shared applications on the smartphone. Furthermore, applications users should be able to inform and correct any data shared if there is a need for modification due to a mistake or a modification. Instructions on how to rectify data should be addressed.

Even if consent is acquired, it is important to check if the data collection is not excessive with regard to consent by collecting more types of data. It is possible that personal data are being collected without being obvious to the developer so external audits can be quite useful in this matter..

5.4 Mobile security best practices
User authentication is of the critical ways to protect what is stored on the mobile phone. Every phone can be locked with a screen lock and use a password, facial recognition, or fingerprint (biometrics) to unlock. Multi-factor authentication is considered one of the best ways to protect users' data that are stored in a smartphone.
Keeping applications and mobile operations systems up to date with the latest security patches is a must. Google and Apple provide updates, at least for the latest smartphone models, on a regular basis to mitigate recent vulnerabilities or threats and improve the security features.

In order to prevent reverse engineering attacks, code obfuscation can be used as a code hardening technique making the code of the application difficult and no timely wise to be exploited.

Back-up on a regular basis is one of the most used ways to prevent data loss. A regular schedule can be applied to ensure data availability, and for mobile devices, a remote backup is common. Although regular back-ups and cloud storage ensure data availability, it depends on the security of the cloud provider and the encryption used during transfer in order to avoid misusage.

Encryption, while the data are stored on the smartphone or during transmission over the network, can ensure the data are protected, and only an authorized party with the required key can decrypt and read the data in their original form.

Enabling remote data wipe on a smartphone is a good solution if a smartphone is stolen or there is a termination of employment. A remote factory reset is executed, erasing all the applications and personal data stored on the phone with few chances for retrieving them.

Awareness of social engineering techniques that focus on the human factor, the user, to take advantage of a person’s feelings, greed or ignorance in order to exploit them and gain elevated access to their information.¹⁴⁰

Strong encryption is highly recommended during storage or data transmission; also, the application notifying the user that data are transferred is recommended.¹⁴¹ Moreover, in a


case of a breach, the competent authority and the user should be informed, and helping the user relieve the consequences of the breach or compensation is possible.

*Isolation of application Information*

The use of a container-based model is highly recommended in order to separate application data from the user's private data. This process requires a few levels of protection but will help to eliminate the risk of data leakage.

**5.5 Secure payment**

Almost 40% of the transactions are completed from a smartphone, while at the same time, almost every application offers in-application purchases for upgrades or additional services. To ensure secure payment mechanisms, appropriate measures should be taken regarding the payment services. Patterns of location and profile can be used to detect suspicious transactions, and after that, re-authentication is highly recommended. Furthermore, whenever an additional cost is required inside the application, the user must be informed transparently and in an easy-to-understand way. At last, each device, operation system, and application store provide different guidelines on how the in-app payments are executed and what additional security measures are required.

Applications that provide in-app payments or are using paid resources of any kind (like NFC) should take extra measures to prevent possible threats that can have a tremendous financial impact on their users. Logs should be maintained and be available to monitor by the end-users while also being protected by unauthorized users. Usage patterns can help detect unusual payments and require a re-authentication, for example, in a case of a significantly higher cost of a usual service or a change in location of the user). Consent for any cost implication should be required\(^\text{142}\), and developers should take into account the different operating systems of the devices. Since operating systems give different access levels into system resources and services even in different versions, access control should be implemented to avoid abuse of the given access. At last, every OS and device vendor has

specific guidelines regarding in-app payments that the developer must follow and take into consideration.

Screen capture, copy, cut, and paste functionalities should be disabled in interfaces that handle sensitive data like banking applications. In the case that a platform does not support this tactic, the user must be informed about the potential security threats such an action can cause.

5.6 Application Developers
Application developers play a significant role in how privacy-preserving and secure an application can be. In order to achieve that, they need to take a lot of measures during the development phase and continuously evaluate and audit their work to make sure it is compliant with the regulations and uses best practices.

There are many challenges for mobile application developers, mainly when an app is used within the EU, which falls into the GDPR compliance. Some of the challenges for the app developers are the following:

- They need to understand the meaning of personal data and privacy and be able to offer protection for both in their application.

- Identification of personal information, where are being stored and offer protection for a limited period

- The ability to distinguish personal data (phone number, location) and sensitive personal data (biometrics) and to be able to provide the level of security needed for each during processing.

- To have a clear understanding of legal perspective about consent, how to obtain it, and its rights to app developers regarding data processing.

- The way consent is acquired should be in a simple language and a clear way; otherwise, it can be invalidated.

- To use the appropriate technical measures in order to offer privacy by design.
Furthermore, in order to be GDPR compliant, an application must ensure the following.\textsuperscript{143}:

- All Personally identifiable information (PII) entered by a user or generated by the application or a third party should be identified, stored, processed, or retrieved accordingly.

- Personal information and data should be protected by sharing with third-party applications.

- Default permissions options should be reviewed and modified.

- The application should include a transparent privacy policy accessible by the user and offer a consent screen and contact information of the DPO.

- To have into ownership written agreements with all data providers evolved into the application.

- Terms and conditions to be clearly displayed.

- On a removal request, to be able to erase all information from storage and inform the third party providers to act accordingly.

Except for all the aforementioned, data developers should follow the upcoming recommendations that address the most important aspects of application development. According to ENISA 2017 and the GDPR, an application developer should take into consideration the following users rights: the right to be informed and the right to access (art 15), the right to erasure (art 17), the right to restrict processing (Art 18), the right to data portability (Art 20), the right to object (art 21), and the rights to automated decision making and profiling (art 22). In order to practice these rights, the overall architecture of an application should be designed to give users the required choices and chances. For example, a chance on how to use their rights and where to get more information about them should be embedded in the application. Furthermore, a user should be clearly informed if there is a limitation on the functionality of the application if there is a permission denial. It

is imperative that the user can delete personal data whenever he or she feels it is appropriate. Changing passwords and pre-configured privacy settings is also critical.

5.6.1 Permissions best practices
Transparency in permissions is required so the user can understand clearly where the application has access and can make an informed decision.

Dependencies should be carefully considered, especially in cases where third-party libraries are included. In a dependent system, the application inherits the permissions of its components like the aforementioned libraries, so additional awareness is required. Moreover, a minimal number of permissions requested for each action is strongly advised in order to avoid access to sensitive information, especially for tasks that do not need it.

Different methods and techniques were introduced to identify the relationships between application functionalities and the requested permissions in order to detect applications that over-request permissions and evaluate their possible risks.

People tend to install applications even with invasiveness permissions because of social pressure. If some of their friends have installed it, they also do it without reconsidering the risks. However, even if users consider the permissions and are in a position to make an informed decision after they have understood the mechanism and the associated risks, they can still not grant permission only to a subset of the requested. It is all or none if they want to use the application. Another problem with permissions is the time the interface appears. Install time permissions are problematic because they are requested before the user installs the application, so they force the user into consenting since he or she has already decided to install the application. If the chance to check how the application works and what it can offer to a user is given and then the permission requests appeared, a more informed decision would be possible. Furthermore, when a user wants to install an application, most of the time skips the warnings and just accepts without even reading them in order to proceed to download and make use of the application. The same applies to policies where the users just accept everything.

5.6.2 Automatic decision making\textsuperscript{145}
Moreover, the right to object to it is an integral part of the GDPR, but in many situations, it is not even mentioned. It is really important that an opt-out option exists and the information about how automatic decision-making works and what kind of service it provides to be known to users. Furthermore, an option to restrict the processing for marketing purposes is also required and, of course, an affirmative action for consent as well as agreeing to the privacy policy and terms and conditions of the application where all the information about automatic decision making should be demonstrated.

5.6.3 Storage limitation
is also a great challenge since the duration of personal information must be defined, and after the duration, personal data must be removed in a way that identification is no longer possible. So if any data have a limited storage period due to specific purposes should be taken into consideration and when it is required, and anonymization to take place for the stored data. If there is encryption, deletion of the encryption key should take place in order to ensure that data are irreversible non-identifiable.\textsuperscript{146}

5.6.4 The right to erasure
should also be taken into consideration when designing an application. Since a user may request the deletion of all personal data stored or processed by the application, the data controller is obliged not only to delete those data but also to provide proof and inform all other responsible parties about the erasure. Revocation of the consent is one of a justified request, and further reproduction of data after deletion is not allowed. So the application should allow the user to erase personal data and information, accounts, and even uninstall the whole application.

5.6.5 Data transmission
Data in transit should always use a safety mechanism like SSL protocol to ensure security during transmission. Self-signed certificates are easy to be tampered with so, in the case of

\textsuperscript{146} Rösch, Daniel & Schuster, Thomas & Waidelich, Lukas & Alpers, Sascha. (2019). Privacy Control Patterns for Compliant Application of GDPR.
an application needing a certificate, a trusted Certificate authority provider should be used. Back-up files must also be in an encrypted format to avoid possible data leakage.

Since physical protection is difficult to be achieved by an application, even though there are some specific applications that can help delete all the important files or perform a factory reset by distance, application developers can implement some measures to improve the overall security of their application. For example, the implication of a strong password or biometrics can help to ensure that an authorized person only accesses the application. Furthermore, locking the application and needing a multi-factor authentication in a case of failed attempts can help improve the physical protection of applications that have to do with sensitive personal data. Although asking for passwords and pin can have a negative impact on a daily usage, such measures can be applied to more specific applications.  

5.6.6 Cross border transfers
Transferring data outside the EU can be done, but it requires a full disclosure. Privacy policies must identify the organization's location and provide contact details of the data controller or their representative inside the EU. Data subjects should be informed of the intention, the reason for the data transfer, and the names of the countries the data are communicated. The statements should be clear and not ambiguous like "any country we do business with." Furthermore, even if the transfer of personal data is transparently addressed, additional measures should be taken; for example, the same level of protection is mandated and ensure appropriate safeguards. These safeguards should be approved by the European Commission, and a copy of the safeguards should be available for the data subject. At last explicit consent and the option to easily withdraw it is required before a transfer has occurred.


5.6.7 *Data portability*  
According to the right to data portability, if data processing is automated and is based on consent, the data subject has the right to obtain personal data in a structured, common, and machine-readable format. So there should be a download form in a standard format like XML for data to be easily communicated and exchanged. All the exchange should also be documented, and the documentation provided after a proper authentication has taken place.\(^\text{149}\).

5.6.8 *Third-party code.*  
Third-party code implementation is a common tactic for application developers since it reduces the time to make and possibly helps them in difficult or time-consuming projects. Nevertheless, third-party frameworks, APIs, and libraries can pose a threat to both security and privacy. By gaining access to user data can result in a leak. So developers should take measures regarding third-party code before implementation but even after the integration. Security updates and patches should be done to third-party frameworks or libraries in the same way with the personal code, therefore as soon as the provider releases them. Thus, having a security report from the provider is really recommended, and if the third-party content creator does no longer support it, this content must not be used. Developers must also use third-party content only from reliable sources and audit them to be confident of the level of security they have. Validation and inspection of transmitted data can help to prevent data privacy concerns.

5.6.9 *Data storage*  
During design, data storage should be classified according to how sensitive data are going to be stored, and accordingly, security measures should be applied. It is recommended that the file encryption should be done by an encryption API provided by the OS or other trusted source since they can provide better security and regular updates. Most of them provide remote wipes and overall increase the security without putting an extra burden on the end-user. All sensitive data should not be stored and cached if they are not in an

---

\(^{149}\) Rösch, Daniel & Schuster, Thomas & Waidelich, Lukas & Alpers, Sascha. (2019). Privacy Control Patterns for Compliant Application of GDPR.
encrypted form. Reevaluation to access authorization based on additional information like location is also a good strategy.

Personal data and sensitive personal data can be stored internally in a device in order to provide functionality even if the device is offline. However, since this information is related to the data subject should either be omitted or if it is necessary for the application to be encrypted with strong encryption. Even if internal storage is protected by the application sandbox and the operational system, storing unencrypted information in the smartphone can result in many privacy risks.

Application developers must ensure what kind of data they have for each customer, ensure they offer secure storage with protection and that all information is in an easily accessible form and ready to be accessed whenever it is needed.

Caches, temporary storage, and shared folders should be considered untrusted and treated as possible threats. Metadata of photos and location can share information in unwanted ways. Deletion of cache data when exiting the application can help. User data and especially sensitive ones like authentication information such as usernames, passwords should always be stored in an encrypted form in order to avoid risk in the event of a data breach.

Ensure that if the application is removed, any user data should be deleted from the device and any other storage medium.

The restriction should be applied to sharing data with other applications installed on the smartphone. Interconnection and data sharing between applications can create many data risks like malware collusion.151


Another important strategy is to minimize the access to sensors whenever it is possible for the necessary function of the application. For example, location data, GPS usage can be diminished, and the exact position would be given approximately since it is not required at all times. By doing so, data minimization is satisfied. The above can be achieved using privacy-enhancing technologies.

5.6.10 Children
Developers should have special considerations and measures, especially if the target audience of their application is kids and teenagers. Kids' and teens' data should be dealt with extreme caution, and it is a good idea to comply with regulations like the Children's Online Privacy Protection Act (COPPA) and the GDPR. Both regulations require parents’ consent and promote an almost bare minimum data collection policy. Additionally, age-appropriate notices are required about the data that are being collected or shared.

As a developer, someone must always stay alerted and informed about new developments since new privacy rules and policies are developing quickly, and the implementation of the new measures should take place as soon as it is possible in order to provide the best security for their consumers and avoid possible fines.

5.6.11 Accountability
is one of the major principles of GDPR and requires application developers to be able to demonstrate with documentation all the procedures they have done, including data protection impact assessments. Furthermore, they need to provide documentation of risk assessments, a record of consents contracts with third parties, and all the security-relevant actions with regard to their application.¹⁵²

It is of paramount importance that users understand the threats that can emerge from using a smartphone application in order to be able to use some security measures that are essential. General threats are mostly familiar, but knowledge about more complex threats that are on the rise is not satisfactory. Users must be aware of safety measures, threats, and the negative consequences in a case of an event. Once a threat becomes a reality and data

are mishandled, it is difficult to return to the previous state; therefore, security and awareness must be utilized beforehand.\footnote{Blaž Markelj, Igor Bernik, Safe use of mobile devices arises from knowing the threats, Journal of Information Security and Applications, volume 20, 2015, Pages 84-89, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2014.11.001.}

A simplified privacy checklist that was able to fit on the main screen of an application description played an active role in user selection. Even the location and the time of the checklist plays a role since it can influence the choice of the users, especially between similar applications. A warning design of privacy indicators helps to inform users of the risks the application might have and help them make a more concerned and privacy-aware choice even for average users. The visual representation of privacy risks is a great tool that can help to inform the consumers and help them make decisions that can lead to a more safe environment.**

Application developers are neither security nor law experts, and since developing an application requires a vast knowledge of the above, the ideal way to improve the applications is communication. Communication can play a crucial role in how knowledge is transferred between parties and can increase collaboration. API designers and providers must work closely with app developers and security experts in order to understand the possible security threats of their own applications and help understand how and when to mitigate them. Furthermore, by this collaboration, developers will be able to clearly understand what their application functionalities want to be and what needs or can be done security-wise. This dynamic approach will help to quickly identify and address security problems resulting in more secure applications.\footnote{P. D. Chowdhury, J. Hallett, N. Patnaik, M. Tahaei and A. Rashid, "Developers Are Neither Enemies Nor Users: They Are Collaborators," 2021 IEEE Secure Development Conference (SecDev), 2021, pp. 47-55, doi: 10.1109/SecDev51306.2021.00023.}
5.7 How can app stores enhance privacy and data protection?

Google Play and Apple store, as the two most used application stores, can help to enhance privacy and data protection in some of the following ways. They can increase developers' motivation to follow more privacy requirements while at the same time highlighting to end-users the benefits and the potential losses due to insufficient security measures or system-level changes. In some situations like the new storage framework that does not allow applications to store files and data in external storage that could remain untouched even if the application is uninstalled, it can result in having users different expectations of the application behavior even if there are clear benefits regarding the privacy and security. In situations like this, the operation system and the application stores can use notices that clearly state the application functionalities. And what could possibly change in a case of an upgrade? Additionally, if the above is framed and demonstrated in a way that promotes security and privacy-preserving features will help users understand better the functionality and develop a more privacy-friendly mindset. Furthermore, with this kind of information will take the burden from developers' concerns about negative reviews due to different application behavior and make the transition to new and more secure frameworks easier.

Except for the above application, stores and operating systems can influence the developer’s choices by introducing new API designs that demonstrate new functionalities and addressing the problems they are trying to solve. Moreover, by highlighting the benefits of switching to this kind of new API will convince the developers to switch to new frameworks and understand better what security measures are important and how they can benefit from such changes.

Another step that can help with compliance is reducing unnecessary hassles for the developers. A clear and comprehensive guide about privacy requirements and how to achieve them can help developers gain a different perspective and save them much time.

---


Additional testing of released software and how compatible this is with privacy regulation and with older versions and different parts of the system can help developers have a better view of how each part works and make more informed choices. In addition, providing an improved OS-level permission system that can help the communication between developers and users and change the review process on the stores can have a positive impact.

At last, a good idea is to find a way to reward developers when they do better at security features. Since managing privacy requirements means a lot of extra work for the developers with very few benefits for them. Privacy-related metrics used in the ranking system can help promote safer applications while at the same time motivating developers to minimize security threats in order to compete better with safer applications with similar features. Furthermore, having users’ metrics about security incorporated in the reviews can also help promote more secure applications and help users make more informed choices about which application to use and install.157

Users should avoid using application stores that are not official and share different versions of known applications, like app stores for rooted devices. Verification of digital signatures of applications can be used to ensure that applications are original and downloaded only from trusted organizations without having their code modified by external sources.

Rating is an important factor when a user considers downloading an application. A privacy rating of an application can play a role in making a decision, but most of the time, the cost of an application is one of the critical factors even for experienced users who can understand the privacy risks. Privacy permissions and ratings can be used to help consumers make a more informed decision regarding installing a new application on their smartphone.158

Organizations should also have an incident response plan according to GDPR requirements to be able to respond to a possible data leak. A data flow mapping is essential in order to keep track of all the personal data a company is handling and be able to conduct audits whenever it is needed.

**Transparency**

In a study where application interfaces were used in order to provide individuals with information about data collection and sharing of common apps. By providing this transparency to users, they purposely find more privacy-preserving applications and use them with more confidence. Lacking control on their data while being tracked had resulted in minimizing the application usage and the installation of new ones. On the other hand, many people were pragmatic. As a result, transparency mechanisms can help users make more informed choices about applications regarding data collection and sharing practices and, by doing so, pressure all actors involved into reforming the standards of privacy and data protection in the whole app market.¹⁵⁹

**5.8 Privacy by design**

Privacy by design (PbD) is a term used a lot in the last years, and it is widely adopted by regulatory frameworks while at the same time questioned by a lot of critics due to implementation difficulties. Privacy by design suggests that the design of the fundamental architecture and features of new technologies, including applications, should be done having privacy in mind.¹⁶⁰ To achieve privacy by design in applications, design strategies have been developed around the following eight factors:

---


1. Minimize, which refers to the limitation of processing personal data as much as possible for the normal functionality of the application.

2. Separate, which prevents the correlation of personal data by separating the process independently.

3. Abstract, which limits the number of details of personal data used. For example, extracting and using commonalities instead of the personal data or using the approximate location of a user for the location services instead of providing the exact coordinates.

4. Hide, which protects and makes personal data unlikable. It demonstrates that prevention of publishing personal data and restriction of unauthorized access using encryption and authentication of even the metadata can help reduce privacy risks.

5. Inform providing data subjects with all the information about the reasons the process is done, which data are being processed, and how.

6. Control provides data subjects with tools and mechanisms that can help them control the processing of their data.

7. Enforce a privacy friendly way of processing data by using privacy management systems and following privacy policies.

8. Demonstrate to be able to provide evidence that the processing of personal data is done in a friendly way having reports and logs while also carrying out privacy and security audits.

Regulators should provide best practice solutions that can help bridge the gap between software engineering and law. Concepts or even some code implementations of privacy-enhancing technologies can help developers adopt more privacy-friendly solutions to their applications and fulfill all the requirements. State-of-the-art solutions can be used in order to provide future proof.

Instructions and discussions can facilitate developers for training and analyzing which are the advantages and potential disadvantages of the techniques they use. Further support towards them and open communication instead of punishment in the form of economic sanctions and fines could result in a community that promotes privacy by design.
It is important that parties who design technologies and platforms on which mobile applications are built and marketed be equally accounted for and provide privacy-friendly functions. Since they can set the bar for additional privacy by default and help developers make more informed choices. Nowadays, developers are constrained by the existing platform rules and technologies like libraries, development kits, and app store review policies. All role-players in this ecosystem must take privacy in a serious manner, and this can only happen with tighter or more specific regulations.

Another aspect of PbD is taking the experience of the users into account at the early stages of the product development in order to avoid privacy risks that might occur later and would be much harder to address\textsuperscript{161}.

The concept of privacy by design is straightforward, to develop technologies that respect the privacy of their users and to develop them from the beginning. However, the implementation of the idea into technology is quite challenging and lacks engineering support.

Both punishment and awards can have a positive impact on promoting PbD implementation because both can result in making engineers more likely to adopt PbD strategies. A top to down approach can be used to promote the implementation of PbD, starting from regulators and executives to engineers and end-users. Like developers having issues about spending time to improve privacy and data protection of their applications without having measurable and countable imminent results. In the same way, engineers could not make direct profits by implementing PbD while it is possible to have performance damages, so evaluation and promotion of the above strategies are required by the top levels and why not

an implementation of privacy can also be added as a performance measurement indicator.\textsuperscript{162}

Furthermore, the development of infrastructure organizational and technical can also support the implementation. With the help of automatic tools that could provide auditing with the lightweight method can result in better and more frequent implementation since adequate support will exist and help them.

At last, the perspective of each individual developer and engineer and his/her awareness has a significant impact on the implementation of privacy by design. So by educating developers and informing them about the process of implementation, offering them better support and tools to work can help them integrate a privacy mindset into their workflow. Furthermore, this is the most important factor to achieve since privacy and data protection is never-ending because it is changing day by day. Therefore all actors should stay informed about the recent trends, have privacy security training and have clear communication, and ask for support or additional education when it is needed.

\textbf{5.9 Regulations}

can play a significant role in how secure applications can become. GDPR implementation was followed by a lot of changes in the whole application ecosystem. Still, mobile and platform manufacturers have a great interest in user's data and take advantage of certain features. For example, a lot of people trust default settings and default applications in a brand new smartphone and never question if these settings are in their best interest. Data minimization article helped reduce these techniques, but still, all the data that are being collected by default are not necessary for the functionality of the phone.\textsuperscript{163}

Regulations should take into account new technologies like Big Data and Artificial Intelligence and react quickly to provide adequate protection for the users. It is important to


note that with the fines imposed to big organizations can strong-arm them in order to take additional measures and provide more privacy-preserving services and products.

5.10 Automation tools
A lot of automation tools have been developed in order to assist developers and users to check applications and identify possible risks. Some of the tools are demonstrated below:

A tool called privacy meter analyzes the permissions an application requires and the privacy risks related in order to provide users with an interface that highlights those risks. A warning display mechanism called the privacy meter evaluates the dangerous permissions of an application and provides users with a visual slider bag making it easy and quick for users to understand the associated risks before installing an application. This technique works as a warning system and helps end-users make more informed choices by understanding how risky an application is and drastically reducing the installation and recommendation of high-risk applications.\footnote{Kang J., Kim H., Cheong Y.G., Huh J.H. (2015) Visualizing Privacy Risks of Mobile Applications through a Privacy Meter. In: Lopez J., Wu Y. (eds) Information Security Practice and Experience. ISPEC 2015. Lecture Notes in Computer Science, vol 9065. Springer, Cham. https://doi.org/10.1007/978-3-319-17533-1_37}

Another tool called Lumen Privacy Monitor is an application that can be used to provide transparency and help users understand how their application handles their personal data. Lumen captures and analyzes the network traffic of a smartphone, including encrypted flows and data. With the examination of the dataset, unique identifiers and personal information are identified and domains that are being contacted by the applications in order to understand if there are third-party domains and services that process users' unique identifiers.\footnote{Razaghpanah, Abbas & Nithyanand, Rishab & Vallina-Rodriguez, Narseo & Sundaresan, Srikanth & Allman, Mark & Kreibich, Christian & Gill, Phillipa. (2018). Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. 10.14722/ndss.2018.23009.}

DroidPatrol is a plugin that can be used by Android developers during application development phases and can help identify potential vulnerabilities. The plugin performs a
static data flow analysis and can detect various security vulnerabilities following OWASP guidelines. By highlighting the parts of the code that can be risky helps developers identify and remove possible vulnerabilities of their application and, in this way, minimizes the potential attack vectors.\textsuperscript{166}

Taintdroid provides real-time analysis and monitors sensitive data by using a technique called "tainting." The application "taints" sensitive information making them easy to identify and track during the use of an application. This can help detect suspicious handling of sensitive data and share it with third parties and advertisement servers.\textsuperscript{167}

Enhanced location cloaking algorithms can be used to hide the location of smartphones while at the same time preserving the locational privacy of the users. With this approach, users can hide their location and time and can still maintain recommendations and services by mobile location-based services (LBS).\textsuperscript{168}

\begin{flushright}
\end{flushright}
6. Conclusions

This dissertation addresses problems that are almost invisible for the average user and the average developer, but have the potential to cause psychological, economical and reputational damage. In this study, we set out to answer the following research questions:

- How do mobile applications implement regulatory requirements of the GDPR, and how compliant are they?
- What are the most common data protection challenges in mobile applications?
- What measures can be implemented to improve data protection and the users’ privacy in the mobile application ecosystem?

We conclude that a lot of applications do not fully comply with the requirements of the GDPR and can impose a data protection risk. Even though GDPR has been implemented for three years by now, there are still applications that process special categories of data without consent and do not provide appropriate security measures when the data are transferred to third-parties, which happen without disclosure. Regarding the consent and the provision of information about the purpose of processing, there are respectable implementations; however, there are many technical aspects regarding the development and the usage of applications that require improvements.

Mobile applications are growing every day and are being used by a far greater crowd. Even amateur application developers are able to create and distribute an application. We identified many challenges regarding data protection in the application ecosystem that are a result of various reasons like technical difficulties or regulation misunderstandings. The acquisition of additional profits using consumers’ data is one of the primary reasons for data misusage.

Successfully implementing the GDPR into mobile applications requires a vast knowledge of the current application ecosystem, development strategies, and regulations. Application developers are not lawyers and have trouble translating the legal requirements into technical solutions. Furthermore, with the rise of citizen developers, there is a lack of technical skills to provide solutions for the countless challenges application development
has. Developers need to constantly audit their application and check if all the appropriate measures are followed.

Where personal data processing is concerned, the discussion focus on privacy and data protection. These fundamental rights have the most direct connection with data processing in practice. However, new technologies and mobile applications can have a long-term effect on people’s lives by their daily usage. It is worthwhile to explore how additional legal approaches would be implemented in technology matters and assist in neutralizing the negative effects that mobile applications can have on an individual's rights and freedoms. Regulators and policy-makers can have a huge impact on the functionality but also on the data protection mechanisms of the applications. Application stores have the power to influence and assist into compliance from the development phase until the distribution and usage.

Another important factor is the end user. As the modern society uses data as a form of currency, the end user must be informed and considered before making any decision regarding the usage of an application and sharing personal data. Privacy risks are challenging to be communicated and many risks evolve and change taking advantage of the rapid evolution of technology. The ease of use, convenience and the rich functionalities of the applications are attributes that influence the choice of the consumer. But on the same time, the excessive invasive behavior and the processing of data play a small part in the decision making process. An effort to communicate the risks and to improve the data literacy of the end users can result in a trustworthy and privacy preserving application market.

We also conclude that there is a need for a holistic approach from users to developers, organizations, and policy-makers to improve data protection and privacy in mobile applications. Ensuring compliance with the GDPR and the confidentiality of a user’s personal data is an ongoing process that has to be embedded into the complete lifecycle of an application. Human factor plays a significant role and it is imperative to educate everyone about the crucial importance of privacy, ways to protect and practice our rights and how to identify data protection risks when using mobile applications.
Limitations

This study has limitations since it is focused on GDPR compliance in Europe. Most of the results are for Android applications since most of the studies are focused on this platform.

Recommendations for Future work

A future research plan might have to deal with the rising of Big Data and the implementation of AI technologies in our smartphones and the many new data protection risks that would emerge. Also, new regulations like the ePrivacy will lead to major changes in the application ecosystem and challenge the way they function and how smartphone applications are going to be developed and used.
7. Bibliography


[16]. Art. 8 GDPR


[38]. European Commission, Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016


[53]. International Organisation for Standardisation/IEC 2382–1-1993


-- 103 --


[122]. T. Timan, Z. Á. Mann “Data protection in technologies”, October 2019. BDVA.


-- 109 --


