A GUIDE TO DATA PROTECTION IN MOBILE APPLICATIONS

2021

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

1.1 Context and scope

Mobile applications, or apps, are software programs developed for and deployed to run on mobile devices such as smartphones or tablets. As a result, they may access and use (depending on operating system and user permissions) data stored on a specific device, such as a contacts list, as well as data from the device's various sensors. According to the former independent European advisory body on data protection, the Article 29 Working Party, these can include: "… a gyroscope, digital compass and accelerometer to provide speed and direction of movement; front and rear cameras to acquire video and photographs; and a microphone to record audio. Smart devices may also contain proximity sensors."[1]

This ability to collect and process data stored on or generated by the device, and potentially combine it with data generated in a specific app, may bring about significant risk to the data protection rights of individual users. Given there were 218 billion app downloads globally in 2020,[i] with chat messenger type apps, social networking apps and entertainment and video apps leading the market,[ii] the capacity for misusing the personal information collected may be high. And the risk to user data protection and privacy may be even higher with health, fitness and nutrition apps; maybe less popular in terms of use, they enable access to more sensitive categories of data such as health status.[2]

The mobile app ecosystem is particularly complex, with many different parties involved in developing and deploying an app on a mobile device. These include, but are not limited to, app developers, app providers (also called 'app owners')[3], operating system manufacturers, device manufacturers, third-party service providers supplying software applications that

---

[1] Article 29 Working Party. "Opinion 2/2013 on apps on smart devices." WP202. *Europa.eu*. Feb. 27, 2013, p. 4. Web. Oct. 29, 2021. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>. The Article 29 Working Party has now been replaced by the European Data Protection Board (EDPB) but its guidelines remain valid as the EDPB endorsed them in 2018. edpb.europa.eu. Dec. 15, 2021. <https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf>.

[2] Health, fitness and nutrition apps had a usage reach of 29.4 percent globally, opposed to 90.7 percent of messenger apps and 88.4 percent of social networking apps. See Statista. "Most popular app categories worldwide during 3rd quarter 2020, by usage reach." *statista.com*. Sep. 7, 2021. <https://www.statista.com/statistics/1252652/top-apps-categories-by-global-usage-reach/>.

[3] ENISA uses the term 'app providers' to describe "… entities that offer the app to end-users or otherwise the 'owners' of the app". This guide will use the same term, to differentiate the role of the app provider from that of the app developer, when the two roles do not overlap in the same person/entity. See *Privacy and Data Protection in Mobile Applications*. European Union Agency for Cybersecurity, Nov. 2017, p. 9. Web. Nov. 21, 2021 <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications>.

mobile app developers integrate into their own apps, and cloud service providers. This guide is intended for app providers and app developers. The same person may perform both these roles, when an app provider who has the initial design idea and offers the app to end-users also designs and develops the app in a technical way. This is not always the case, however. Often the person who has the design idea will lack the technical skills to create the code for the app's functionalities, and will contract an external party to develop the app on their behalf. Identifying the various roles and understanding their importance is essential in determining how data protection responsibilities and liabilities are allocated; that is, who is responsible, and for what. With regard to data protection, usually the person assuming the role of controller of personal information/data will bear most of the data protection obligations. The person assuming the role of processor will mainly be processing personal data on the controller's behalf, though they may have some direct obligations as well. This allocation of responsibilities may differ between countries but knowing the fundamental principles of data protection[iii] will help you ask the right questions when developing an app or navigating the law of your own jurisdiction.

Data protection rights may also overlap with intellectual property (IP) rights, and it is important to consider both from the outset. For example, a customer database may be protected by copyright, and in some jurisdictions, such as the European Union, by the *sui generis* database right. But it may also contain personal data, and sometimes sensitive personal data, and thus a customer will have rights regarding that data.[iv] Consequently, when creating a database, app providers/developers should bear in mind that processing such personal data is allowed only under specific rules in data protection law. In addition, an app's code may be protected by copyright, and algorithms protected as trade secrets.[4] Using such code and algorithms to process the personal data of individual people – whether users of the app or not – means that app providers/developers must have some understanding of the rights these individuals have under data protection law, and how these rights may interact or conflict with their own or third-party IP rights (see section 5 for the balancing exercise app providers must perform when responding to individual access or portability requests). Moreover, the ability to enforce infringement of IP rights may also be contrary to compliance with data protection principles; for example, storing an individual's personal data indefinitely just to identify them in future IP infringement investigations would conflict with the storage limitation principle (see section 4).[v]

This guide complements the WIPO series of IP-focused tools that assist providers/developers use IP rights to protect their apps. It aims to help app providers/developers understand their

[4] For how to protect your app using IP, see Shemtov, N. "Protecting your mobile app." *wipo.int*. 2021. Web. Nov. 29, 2021. <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1071.pdf>.

data protection obligations, how to comply with them, and how they may occasionally conflict with their IP rights. Data protection compliance is an important legal issue in its own right and should be considered at the start of the app development process, as the consequences of noncompliance may include high administrative fines and/or criminal penalties.

This guide does not focus on a particular jurisdiction or national legislation but seeks to raise awareness and provide practical guidance to mobile app providers (and mobile app developers, where the same person performs both roles) on fundamental data protection and privacy issues arising from the design, development and use of mobile apps. Nevertheless, it loosely uses the European Union General Data Protection Regulation (GDPR) as inspiration for structure and discussion for two reasons.[vi] First, the GDPR has a broad extraterritorial effect, in that it applies not only within European Union borders; companies based outside may still be subject to the GDPR if they target individuals in the European Union. Second, many countries, including Brazil, Japan, Kenya, Nigeria and People's Republic of China (PRC),[vii] have been inspired to draft their own data protection legislation in line with some of the principles of the GDPR, even if the constitutional background, application of rules and enforcement by competent authorities differs. Where appropriate, there are references to specific examples from jurisdictions around the world.

Due to its brevity, and the need for a general overview of the most important issues relating to data protection in mobile apps, this guide is neither exhaustive, nor provides in-depth analysis. However, there are references to a number of other opinions, guidelines and resources, if further reading is required. Finally, please note this guide and the practical tips included herein are for information purposes only and should not be construed as legal advice. Responsibility for views expressed remains solely with the author.

1.2 Privacy and data protection: similar but different rights

Even though the right to privacy and to data protection appear similar, they do not protect the same activities. On the one hand, the right to privacy in some jurisdictions protects an individual's private and family sphere and the confidentiality of their correspondence;[viii] in American law history, it has famously been coined 'the right to be let alone'.[ix] For example, the right to privacy may protect the confidentiality of an instant messaging communication whether or not this includes any personal information/data. On the other hand, the right to data protection applies to individuals in relation to the processing of their personal data; thus, if data are not personal, the right does not apply. For example, this is the case when data have been anonymized in a way that can no longer identify individuals.

The protection provided by each of these rights may be broad and cover a range of circumstances. You may think the right to data protection is more narrow as it protects individuals only in relation to the processing of personal data, but often the definition of what constitutes personal data is extensive and the protection may extend to data that have become public; data may no longer be confidential, but may be still protected, as long as they fall under the definition of personal data.[5] As a result, an understanding of which data are or may be personal is essential.

Due to its brevity, this guide focuses only on issues of data protection.

1.3 Why is it important to think about these issues?

When considering developing a new app, key data protection issues may not seem a priority, given the costs associated with implementing data protection policies in the app development process. This is particularly the case when developers/providers are not part of a big company with access to legal and technical resources. But if processing activities are subject to a jurisdiction where organization size does not matter when it comes to data protection obligations, a single developer will be subject to the same rules on fines as larger organizations, sometimes even criminal penalties.[x] Therefore, thinking about these issues from the outset, and integrating data protection in the app development process, may be economically beneficial in the long term and save time.[xi]

Many countries have enacted data protection legislation that empowers competent authorities to investigate data protection violations, and depending on the jurisdiction, impose fines that may be extremely high.[xii] Beyond avoiding fines, incorporating data protection policies when building apps may provide a competitive advantage and enhance the app's reputation, as well as mitigate any risks to consumer trust when something goes wrong, such as a data loss or breach.[xiii]

[5] Protecting publicly available information may be the case under EU data protection law but not under other jurisdictions; e.g., the California Privacy Rights Act 2020, sect. 1798.140, on Definitions (v)(2) defines when publicly available information is not considered personal information. See IAPP. "The California Privacy Rights Act of 2020." *iapp.org.* Mar. 2021. Web. Nov. 2021. <https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/>.

2. DOES DATA PROTECTION LAW APPLY TO THE PROCESSING DONE BY MY APP?

2.1 Material scope

As data protection law will apply to the processing of personal data, it is essential to understand what data are or could be personal. Generally speaking, personal data are data that relate to an identified or identifiable, living, individual person. This definition may be broad and include data such as identification numbers, online identifiers, IP addresses, device identifiers and location data. Examples of personal data include a person's name, phone number, email address, postal address and photos. In European Union law, where the definition of personal data is particularly broad, it may also relate to a person's "…physical, physiological, genetic, mental, economic, cultural or social identity…".[6] In some jurisdictions, there is a specific term for the individual person to whom personal data relate; that person is called a data subject.[xiv] However, as this may not always be the case, the term individual is used in this guide. The term processing is also broad and refers to any operation performed on personal data, from collection to destruction or erasure, including the process of anonymization.[xv]

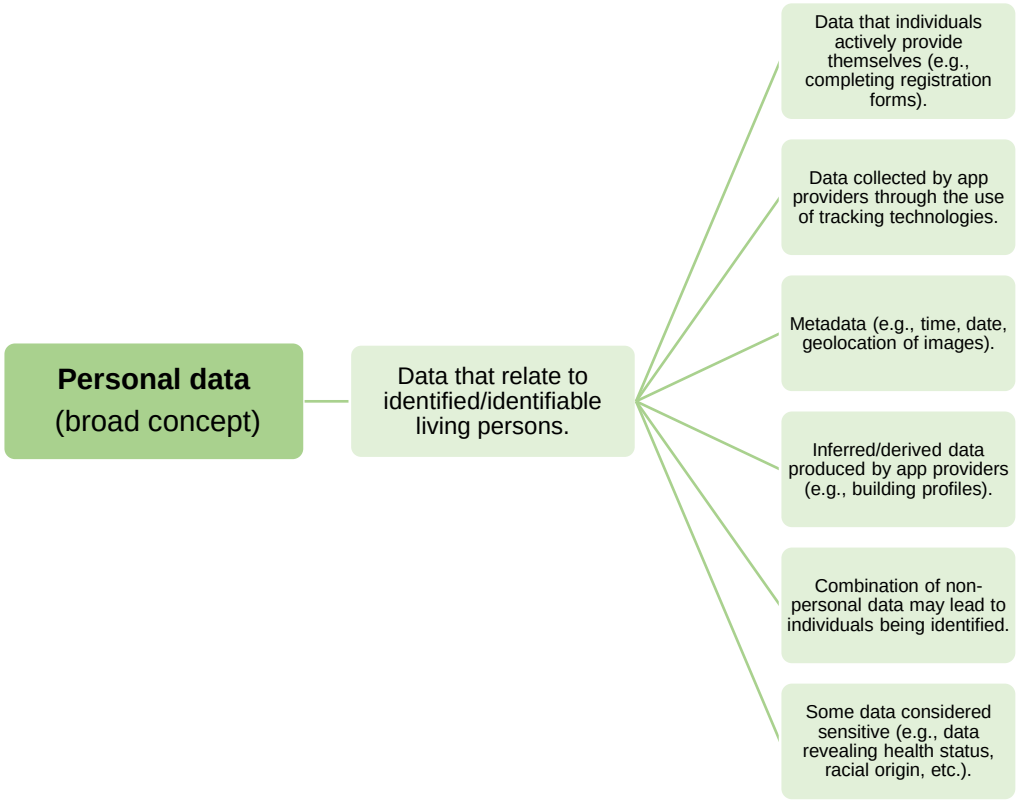
The term identifiable means it is not always necessary to be able to identify an individual directly from the data but it may be possible to single them out.[xvi] This can happen when different pieces of data are combined, and lead to a person being distinguished from other people and identified. For example, processing a combination of data such as an individual's age, profession or postcode could lead to an individual being picked out from others.[7] In some jurisdictions, the law differentiates between personal data and a subcategory of personal data called sensitive data, and may impose stricter rules and obligations for processing such data, which may reveal a person's health status, racial or ethnic origin, political opinions or trade union membership, philosophical or religious beliefs, sex life or sexual orientation, or genetic and biometric data.[8] It is important to remember that data that may seem personal initially could actually be sensitive data if it reveals a sensitive characteristic. Messages exchanged via instant messaging apps may reveal a person's health status or sexual orientation, for

[6] General Data Protection Regulation. "GDPR." *gdpr-info.eu*. Art. 4(1). <https://gdpr-info.eu>.
[7] Article 29 Working Party. "Opinion 4/2007 on the concept of personal data." *europa.eu*. June 20, 2007, pp. 12–13. Web. Nov. 21, 2021. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.
[8] See GDPR, Art. 9(1).

instance, or photographs shared on social networking apps, a person's racial origin or religious beliefs.[xvii]

In addition, metadata (data that describe other data), such as the time, date and geolocation information of an uploaded photo, or observed data about a person's preferences or behaviour, which are collected and processed continuously, could lead to intrusive profiles being built of people that reveal sensitive information.[xviii] Moreover, combining different sets of data, even anonymous data that are not initially subject to data protection law, could ultimately reveal personal (or sensitive) information on a person, and thus the combined data would be treated as personal. When making such assessments in data protection law, context is everything, requiring a case-by-case approach.[xix] See figure 1 for examples of different types of data that could be considered personal.

Figure 1: Types of data that could be considered personal data



2.2 Territorial scope

Territorial scope may refer to two important questions: how app providers and developers know which data protection law applies to their processing of personal data; and whether there are any data localization requirements, meaning personal data must be processed only in a particular country and must not be transferred out of that country.

First, occasionally it may not be obvious which national data protection law applies to a specific processing of personal data. Different jurisdictions may use different criteria to determine whether their laws would apply. It may be that the important criterion is where the app developer or provider is established, irrespective of where the actual processing takes place, or in the absence of the establishment link, whether they offer and target their services at individual users who are citizens or residents, or simply present in a particular jurisdiction.[xx] So, depending on circumstances, you may need to consider the data protection law of the country where your company is established, and the data protection law(s) of the countries where the individual users of the app are located or where processing takes place.

And second, it is important to know whether personal data must be processed only in a particular country, or whether personal data are allowed to be transferred outside that country or jurisdiction. Some jurisdictions, such as the European Union, Russia Federation and Saudi Arabia, impose strict requirements on data transfers, which may be allowed only when there are sufficient safeguards and guarantees that the third country where the data are transferred will provide an adequate level of protection with regard to individual data protection rights.[xxi]

If app providers/developers use third-party service providers to integrate additional app features, such as advertising or analytics services, or use cloud providers for external data storage, it will be important to know where such providers are located. If outside the app provider/developer's jurisdiction, transferring data to them in their country may be considered a data transfer under data protection law and be subject to specific processing requirements. This is an issue that should be included in contractual agreements between app providers and developers, and third-party service providers, along with a description of the specific safeguards implemented to legitimize the transfer; for example, specific contractual measures. In this context, some cloud providers offer customers the option to store their data in data centers located in specific regions, or commit to using subcontractors located only in specific regions.[xxii]

3. THE MOBILE APP ECOSYSTEM: RISKS, ACTORS AND OBLIGATIONS

3.1 Privacy and data protection risks specific to mobile apps

When assessing the privacy and data protection risks for individuals through the use of mobile apps, understanding the context where processing takes place is important to identify the sources of risk, and the potential impact of the processing on the individual, and the limitations to implementing mitigating measures to prevent those risks materializing. Apps may be created to provide a specific functionality (gaming or fitness apps, for instance) but may also integrate third-party services. These could be social networking features allowing users to share their data, such as their gaming scores or daily exercise activities. There may be higher data protection and privacy risks when an app integrates a social networking feature or third-party advertising services because of the potential sharing of data between the app developers and the third-party service providers. In addition, there are different data protection risks arising if an app targets adults rather than children, as some jurisdictions have stricter data protection rules for processing the data of minors.[xxiii] Further, if an app is addressed to minors, the app environment and advertising targeted at them should be suitable for their age group.[xxiv]

Essentially, complying with data protection law, and being able to demonstrate compliance to competent authorities or individual users, may require a privacy or data protection impact assessment (DPIA). This assessment is required by law in some jurisdictions if the processing may result in high risks for individual data protection rights. We look at this compliance mechanism in more detail in section 6.

According to the European Union Agency for Cybersecurity (ENISA), there are two key sources of risk with mobile apps, which it classifies as "…a) their nature, as software running on private mobile user devices (handheld devices), and b) the particularities of the mobile development and distribution environment as such…".[9] Handheld devices have a number of features that may give rise to risks for individual users. ENISA maintains these may relate to devices being imbedded with a number of sensors, which enable a variety of personal or sensitive data to be collected. According to ENISA, these devices are "almost always activated" and include different identifiers, including device ID, metadata and geolocation data, which may enable tracking of the device and individual users across different devices or apps. Moreover, ENISA states their mobile nature makes them more susceptible to physical security

[9] ENISA, "Privacy and data protection", p. 11.

vulnerabilities, and they have “limited user interfaces”, such as smaller screens, that may hinder provision of information to users in an accessible way.[10]

The second source of risks relates to the number of different actors involved in developing and deploying mobile apps (app developers, app market providers, third-party libraries, cloud providers, for instance), and the fact that app developers depend on those parties to offer their app to individual users. App developers may have no control over what the European Data Protection Supervisor terms the “underlying software layers” of device and operating system manufacturers, and thus, may have limited control over “personal data processing and the configuration capabilities of services provided through the mobile application”.[11] Depending on their technical and security expertise, different actors may implement varying degrees of security and privacy policies, and may process personal data for their own purposes, which often may be hidden or not understood, not only by individual end-users, but also by app developers themselves.[xxv]

These particularities of the mobile app environment have an impact on how app developers/providers comply with the data protection principles and other processing requirements. In the next section, we look at who the actors responsible for such compliance are before examining the ways in which they can comply.

3.2 Controllers, processors and their data protection responsibilities

3.2.1 Controllers

The two main actors responsible for personal data processing in data protection law are the controllers and the processors.[xxvi] A controller is a natural person (an individual), organization or other body determining the purposes and means of the processing; the why and how personal data are being processed.[xxvii] There may be more than one controller determining the purposes of a particular processing operation or deciding the means of processing –

[10] Ibid., pp. 11–12.

[11] European Data Protection Supervisor. “Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions.” *Edps.europa.eu*. Nov. 2016, p. 6. Web. Nov. 21, 2021. <https://edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_mobile_apps_en.pdf>.

whether to use a particular service or software to process personal data, for instance – in which case they may be joint controllers. If so, these joint controllers should have an agreement, perhaps in the form of a contract, stipulating their respective responsibilities regarding the processing of personal data.[xxviii] Such a situation may arise between an app provider and a third-party service provider supplying in-app advertising services, or between an app provider and an app store marketplace provider.

In the mobile app context, the person or organization offering the app to the public (the app provider) will probably be the controller of personal data, as they determine the purposes for which personal data are collected through the app, and further processed, and the manner used to process. For example, if an app is developed with the purpose of tracking brain performance through a series of different games (such as games testing memory, language, mathematics, problem-solving skills), and you have to pay to unlock more premium games, then personal data will be processed for a variety of purposes, including registration and instalment of the app, billing and system security, and for tracking performance and creating a unique profile on daily progress. Whether this processing takes place on the individual end-user's device, or whether the data are processed in an external cloud service to scale up data analytics services, depends on which 'means' the app provider chooses to process the data. The means may also refer to which app store the app provider chooses to deploy the app. Even though the app provider is not involved in the design of a cloud service or an app store marketplace, and has made no determination on the way these services function, the fact they choose to use them to process personal data is sufficient to amount to a "determination" of the means of processing.[xxix] If the app provider does not agree with the way processing is carried out in those services, they must decide whether to use the service or request changes to the way personal data are processed.[12]

According to the Article 29 Working Party, apart from the app provider, operating system and device manufacturers could also be controllers when they access and process an individual's personal data for their own purposes, "such as the smooth running of the device, security, etc. This would include user generated data (e.g. user details at registration), data automatically generated by the device (e.g. if the device has a 'phone home' functionality for its whereabouts) or personal data processed by the OS or device manufacturer resulting from the installation or use of apps."[13]

---

[12] European Data Protection Board. "Guidelines 07/2020 on the concepts of controller and processor in the GDPR." Version 2.0. *edpb.europa.eu*. Jul. 7, 2021, para. 30. Web. Nov. 21, 2021. <https://edpb.europa.eu/system/files/202107/eppb_guidelines_202007_controllerprocessor_final_en.pdf>.

[13] Article 29 Working Party. "Opinion 2/2013 on apps on smart devices", p. 10.

Moreover, where the app provider allows access to or shares personal data generated through the app with other third-party service providers – for them to provide advertising based on behavioural data collected from the end-users, for instance – these third-party providers will be controllers, as they process personal data for their own purposes and determine the means through which they process it. For example, they decide to use the particular app to collect the personal data in question. It is important app providers keep this in mind, as in such cases, they may be considered a joint controller with the third-party service provider and be required to have an agreement with them to allocate respective responsibilities regarding the processing of an individual's personal data. Whether this agreement is legally required or has a specific legal format (a contract, for instance) will depend on the specific jurisdiction the two controllers are subject to.

3.3 Processors and controller-processor agreements

If the app provider is the same person/organization as the app developer, the same considerations regarding controllers will apply to the app developer. Where the two roles do not overlap – because the app provider does not have the technical expertise to develop the app and outsources this activity to the app developer, for instance – whether the app developer has a role in data protection law will depend on the circumstances. For example, if the app developer creates the app on behalf of the app provider and then processes personal data on behalf of the provider (for app testing purposes, for instance), then the app developer will be a processor. In contrast, if the app developer develops the app and then steps back and does not process any personal data, then the app developer may not be subject to data protection law. Interestingly, in European Union law, even entities that are simply producers of apps, and thus not subject to data protection law, are encouraged to take into account the right to data protection when designing services or apps, to ensure controllers are able to comply with their data protection obligations.[xxx] This principle of designing data compliant services is discussed in section 6, under data protection by design, and by default.

A processor is a natural person (that is, an individual), or an organization, or any other body that processes personal data on behalf of the controller. Their main characteristic is that they follow the instructions of the controller regarding the purposes and means of processing, and do not make those determinations themselves. If a processor goes beyond the instructions of the controller and starts determining the purposes and means of processing, then that

processor becomes a controller and assumes all the obligations that controllers have. In the case of the app provider/app developer relationship, where the two roles are not performed by the same person, the app developer must develop the app in the manner prescribed by the app provider. Similar to the agreement an app provider may have when acting as a joint controller with other entities in the mobile app ecosystem, an app provider acting as controller may be required to have a contract with the entities acting as their processors.[xxxi] This contract would describe the specific nature, type and duration of the specific processing operations, and include other clauses describing the respective rights and obligations of the parties.

Depending on what is included in the contract (according to the jurisdiction), processors will be liable to controllers for the way they process personal data. They may also be liable to controllers for any failures of their own sub-processors (for example, subcontractors acting as processors) to comply with their respective data protection obligations. This ensures that no matter how complex and layered the processing supply chain may be, the initial processor remains liable to the controller. It may be, however, that it is the controller who is ultimately responsible for complying with the fundamental principles of data protection and responding to individuals when they try to exercise their data protection rights. This ultimate responsibility assigned to the controller is called the accountability principle, and means the controller must not only comply with their data protection obligations but also be able to demonstrate such compliance in practise; for example, when required by competent data protection authorities.[xxxii]

We look at the different ways a controller (app provider) may demonstrate compliance in section 6, but these may include the following:

- Implement internal policies to identify processing operations and map data flows.[14]
- Keep records/logs of processing activities.
- Carry out security and data protection audits of internal processes and processors' activities.
- Conduct data protection (and privacy) impact assessments.
- Appoint a data protection officer who independently advises on data protection compliance.
- Provide training to employees/other persons processing under the authority of the controller on data protection issues.

[14] qLegal. "The impact of GDPR for start-ups: a UK perspective." *qlegal.qmul.ac.uk*. May 9, 2019, p. 2. Web. Nov. 10, 2021. <http://www.qlegal.qmul.ac.uk/media/law/docs/The-Impact-of-the-GDPR-on-UK-Start-ups-Toolkit.pdf>.

- Adhere to codes of conduct specific to the controller's industry if these have been developed.

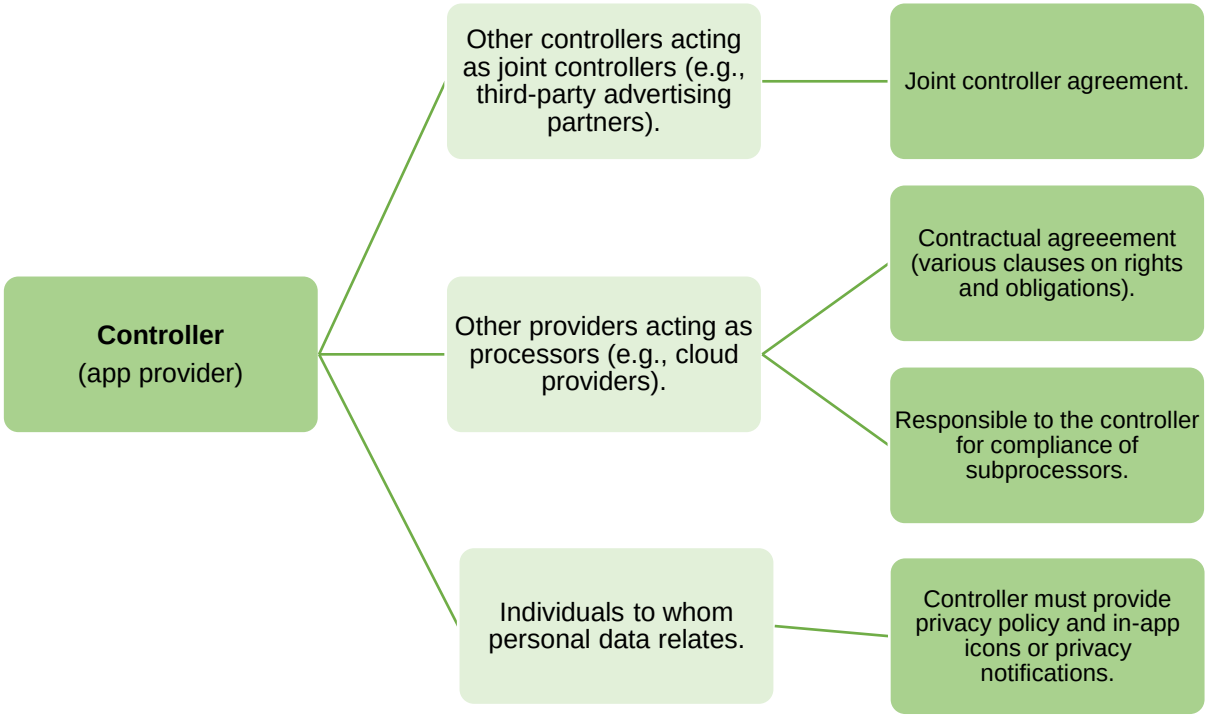
In some jurisdictions, some compliance initiatives are actually obligations imposed directly on the controller or the processor (or both) by data protection law. For example, in the European Union, the controller and processor both have an obligation to keep records of processing activities,[xxxiii] and may be required to carry out a data protection impact assessment and appoint a data protection officer depending on the level of risk for individuals arising from their processing activities.[xxxiv]

Given that outsourcing the development of an app to an external entity requires the app provider to consider how to protect and retain all their legal rights (such as the IP rights on the code, functionality, design and trademark of the app), it should not come as a surprise that the app provider may be required to conclude a contract with its processors relating specifically to data protection compliance considerations. It should be noted, though, that irrespective of how this contract allocates the controller/processor role and responsibilities, what matters is what happens in practise. Thus, a contract may stipulate that a party is a processor, but if in reality that party is processing personal data for its own purposes, it will be considered a controller for that specific processing activity.

Depending on the jurisdiction, controllers and processors may have similar obligations, or controllers may have more onerous obligations than processors, given that controllers have more influence over the purposes of personal data processing. The next section focuses on the obligations of controllers, and their impact on the relationship between controller and processor (for example, the relationship between an app provider and app developer or any other third-party service provider). The focus is on the obligation to comply with the fundamental principles of data protection law, to respond to individuals when they try to exercise their data protection rights and remedies, and to demonstrate compliance. Section 6 revisits the question of why it is important for controllers (and processors) to implement measures to comply with their data protection obligations, and section 7 summarizes the key takeaways.

See figure 2 for a summary of the main relationships between an app provider acting as a controller and some of the other stakeholders in the mobile app ecosystem.

Figure 2: Relationship between app provider and stakeholders in the mobile app ecosystem

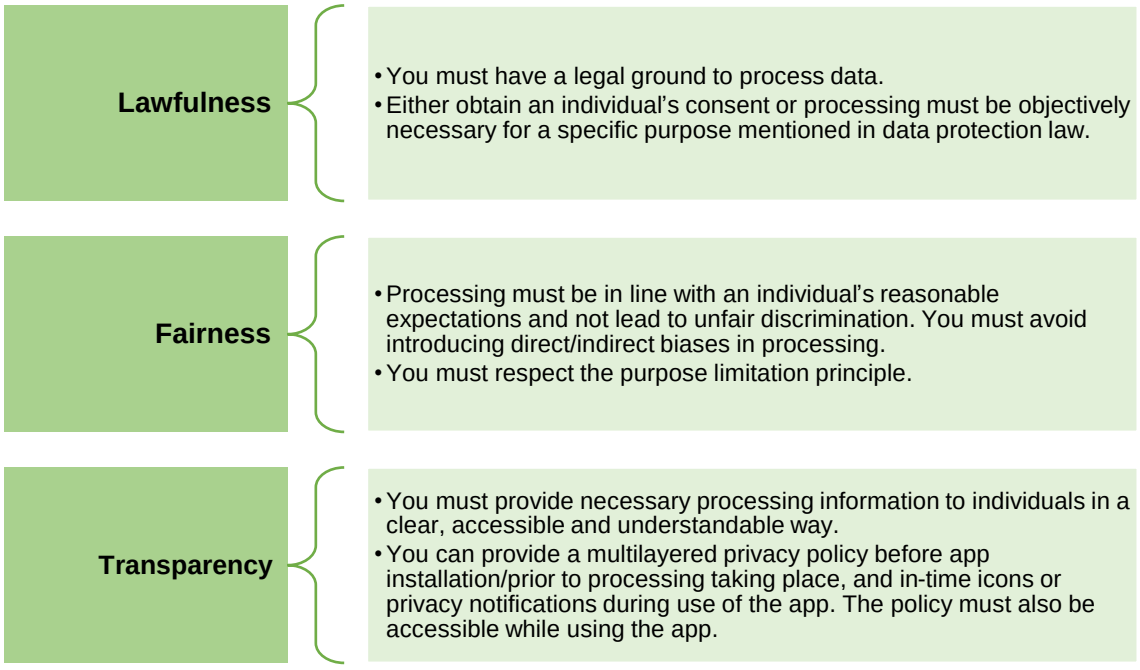


4. DATA PROTECTION PRINCIPLES

4.1 Lawful, fair and transparent processing

Some of the most important elements of lawful, fair and transparent processing, the first principle as outlined in Article 5 of the GDPR, are summarized in figure 3, along with what you, as the controller, can do to comply (see section 4.1.1 for more detailed information).

Figure 3: The principles of lawfulness, fairness and transparency



4.1.1 Lawful processing and legal grounds

A number of data protection laws around the world include provisions on data protection principles.[xxxv] The first principle controllers should comply with is that personal data processing is lawful, fair and transparent. Lawful processing is that which takes place in accordance with the applicable law that sets out the specific grounds on which the controller may rely to process personal data. Those grounds represent alternative options for the controller. There is no hierarchy between the grounds, unless the law to which the controller is subject states otherwise. For example, a privacy-related law may require that for certain services – publicly available electronic communication services such as messaging apps, for instance, or when

specific technologies such as placing cookies on devices are used to collect data – the consent of the individual end-user is required.[xxxvi]

As lawful grounds for processing may include several options for data controllers, generally controllers may obtain an individual's consent to the processing of their personal data, provided such consent is: freely given; specific as to the purposes of processing; informed, in the sense that individuals have all the necessary information about the processing operations before giving their consent and the information that it is their right to withdraw this consent at any time; and given in a clear and affirmative manner, so there is no doubt that the individual intended to consent to such processing.[xxxvii]

Consent to processing should be given prior to the collection and processing of personal data. At the same time, providing consent may be a dynamic process if the purposes of processing change or evolve over time. For example, this would be the case if, after the user installed a mobile app and provided consent for specific purposes, the app provider/developer wanted to incorporate additional features that required the processing of other types of personal data and/or for different purposes than originally thought. Think of a mobile app developed initially to provide general city map directions without the need to collect an individual's precise location data; if this app later integrated a feature showing individual end-users where the nearest bicycle station or bus/metro station was in relation to their location, or offered them the possibility to book a private taxi ride using their location, individuals would need to again provide consent in relation to the processing of their location data for these additional purposes. This presupposes the app provider/developer would need to be transparent as to the types of data collected and the purposes of processing. This obligation to provide transparency and the challenges faced by app providers are discussed below.

These requirements mean an app provider/developer may find it difficult to demonstrate that an individual's consent was obtained in a valid way, particularly when processing sensitive personal data that may require a higher standard of consent, with this being given in a separate, explicit[15] statement (in some jurisdictions).

Additional lawful grounds the controller may rely on include processing that is necessary:

- for the contract between the controller and the individual to whom personal data relate;
- for the controller to comply with a legal obligation (tax, human resources responsibilities, for instance);

[15] Term used in GDPR, Art. 9(2)(a).

- to protect the vital interests of the individual (only when the individual to whom the data relate is physically or mentally incapacitated);
- for the performance of a task carried out in the public interest; or
- for purposes of the legitimate interests of the controller (for example, maintaining system security).[16]

Relying on the last ground will require the controller to balance legitimate business interests against the individual's data protection rights, and decide which are more important. This is a case-by-case assessment. In European Union data protection law, for instance, children's rights may override the controller's legitimate interests under some circumstances.

The common characteristic between these lawful grounds for processing is that it must be necessary for the specific purpose for which it takes place. Considering the main focus of data protection law is to protect individuals' personal data, the term necessary is interpreted narrowly, meaning the processing must be strictly necessary in the circumstances. So, for instance, an app provider offering a banking and financial services mobile app may rely on the lawful ground of "processing necessary for the performance of a contract" to collect the bank account details of the individual end-user and other individuals to whom a payment must be made, as that data are strictly necessary for the core functionality of the app. Without processing that data, the app cannot function. But if the app required users to add a portrait photo in order for a transaction to be approved, that personal data would not be necessary for the service provided, and the app provider would need to have another legal basis to process that data. This concept of what processing is strictly necessary will be discussed further in the section on the principle of data minimization.

Finally, it is important to note that in some jurisdictions, data protection law may impose stricter requirements for the processing of certain categories of personal data, such as sensitive data.

4.1.2 Fair processing

In addition to being lawful, processing of personal data must also be fair, meaning the processing should not be done in a way contrary to the reasonable expectations of the individuals to whom the data relate.[xxxviii] Reasonable expectations will vary according to the specific context; processing for a particular purpose may be fair in one case and unfair in another, depending on the circumstances. This concept of fairness is closely linked to the principle of purpose limitation discussed below, whereby personal data should not be processed for purposes other than the ones collected for, unless the new purposes are closely

[16] These lawful grounds are consistent with those listed in GDPR, Art. 6(1).

related to the original ones, meaning personal data should not be processed in unexpected ways.

Imagine, for instance, a music mobile app that collects personal data on individual preferences in different music genres and artists. Individuals may expect the app will track their music preferences to recommend similar type songs or artists that may be of interest. If data on preferences was then analyzed by the app to predict an individual's age group (someone who listens to music from the 1970s may be over 50 years old, for instance) and target them with age-specific dating advertisements, that would be a hidden, unexpected and thus unfair processing of personal data. Preventing this unexpected processing could be achieved by implementing the principle of data protection by default, whereby the default settings of the app allow the processing of personal data only for specified purposes and not for sharing with third parties. The principles of data protection by default (and by design) are discussed further in section 6.

Moreover, complying with fair processing means that processing of personal data should not result in unfair discrimination of individuals based on one of their protected characteristics (racial or ethnic origin, religious beliefs, political opinions, sex or sexual orientation, among others) in the relevant jurisdiction. Occasionally, processing may lead to unfair discrimination because there is processing of indirectly biased information. This may occur when seemingly irrelevant information is being processed in a way that reveals a protected characteristic and discriminates against a particular group of people.[17] For example, in the context of shopping apps, analyzing the history of an individual user's purchases may reveal information about their sex or whether they identify as male or female. If the evaluation of such information that indirectly reveals a person's sex or gender is then processed to ensure that certain products or services are not offered to an individual, this may lead to unfair discrimination of that individual. App providers/developers should be aware of these risks and potential consequences, particularly as in the mobile environment, data generated in the app may easily be combined with other data on the device and build detailed profiles of individual users that reveal sensitive information about them.

[17] Introducing indirect bias in the processing of personal data may be a problem when using machine learning algorithms for data analytics and predictions. See Kamarinou, D. et al. "Machine learning with personal data." Queen Mary School of Law Legal Studies Research Paper No. 247/2016. *papers.ssrn.com*. Nov. 7, 2016, p. 16. Web. Nov. 21, 2021. <https://ssrn.com/abstract=2865811>.

4.1.3 Transparent processing: privacy policies

The third element of the first data protection principle is that processing of personal data must be transparent. Transparency refers not only to whether the necessary processing information is being provided, but also to whether the manner in which it is provided is transparent, thus the information must be presented in a clear, accessible and understandable way. This means it is not sufficient to provide the information; the app provider/developer must be able to demonstrate it has made an effort to impart that information in a meaningful way to the specific target audience the app addresses. In this light, the language used is also relevant. Language used to address children, for example, will not be the same as that used for older persons.[xxxix] As emphasized at the outset, context is extremely important in personal data processing.

As outlined in the GDPR, for instance, controllers (for example, app providers/developers) must provide information to individuals on the nature, type and context of their processing, including: whether they are processing personal data; which personal data are collected and for what purposes; how long data will be stored for; who is responsible for processing their data (who is the controller); with whom such data are shared or to whom they are disclosed (app providers may allow app store providers access to the personal data on their mobile app to conduct analytics); whether an automated decision-making system is used; and what are the consequences for individuals.

They must also relay how they comply with their obligations under data protection law, including whether they transfer personal data outside their specific jurisdiction and the measures they have taken to ensure personal data are protected. Additionally, individuals must be informed about their rights, how to exercise them, who to contact and how to submit complaints. Whether this obligation to provide information is imposed only on controllers or also on processors depends on the specific laws applying to the processing of personal data.

Even though the law may not prescribe the exact format in which this information must be provided (what type of document is required), controllers usually include this in publicly available documents, commonly called privacy policies. As a privacy policy must include all relevant information on the processing of personal data, it may unavoidably be a long, detailed legal document. Individuals may therefore find it difficult and time-consuming to read, particularly on a mobile phone screen. One way to address these issues would be to provide a multilayered policy,[xl] whereby the first page (layer) includes the most important information with links to subpages providing more details or information about specific technologies (for example, use of cookies to collect data) or processing operations (details on advertising policies, or sharing data with operating system manufacturers or app store providers). Empirically, policies including detailed and specific terms have been found to offer better

transparency, such as those that stated explicitly which lawful ground of processing the controller relied on to process personal data, and for what particular purpose.[xli] For example, an app provider may say it relies on consent to process an individual's location data to offer them location-based services, or on the fact it is necessary for the provision of services when it processes credit card details to authorize in-app payment transactions. Specific descriptions of why processing takes place enables individuals to check its lawfulness and understand their rights in relation to a particular processing operation (for example, they may wish to withdraw their consent to the processing of location data at a later time).

This information must be provided prior to the processing of personal data, and if possible before the app is downloaded from an app store and installed on the user's device.[xlii] For this reason, the privacy policy must be easily accessible at all times, either via the app store where the app is being offered or a link to the app provider's privacy policy,[xliii] or via the app itself while individuals are using it. Personal data processing is a dynamic process, and the obligation to provide information does not end at the pre-installation stage. As processing purposes may evolve over time, or certain app features (such as sharing data with other users via social networking apps in a private or, more so, a public way) give rise to more risks for data protection rights, providers should adopt privacy-friendly designs and interfaces to notify individuals about processing while they are using the app. For example:

"use of context-specific, short privacy notices or icons that appear as and when individuals are about to interact with a provider's service, or with each other may be a user-friendly technique to convey important privacy information found in unitary or multi-layered policies."[18]

More specifically for the mobile app environment, in addition to multilayered policies and icons, the Article 29 Working Party has suggested that providers could employ "images, video and audio…," and use "contextual real-time" alerts when an app accesses contacts or photos,[19] such as "the warning icon for geolocation processing used on iPhones."[20] Providing meaningful transparency is not easy, particularly in complex mobile app ecosystems where personal data processing may be hidden even from providers themselves. By using these data protection-friendly features, app providers may demonstrate in a practical way compliance with their transparency obligations, and that they have considered and implemented the principles of data protection by design and by default during the app development process.

---

[18] Kamarinou, D. et al. "Privacy in the clouds: an empirical study of the terms of service and privacy policies of 20 cloud service providers." Queen Mary School of Law Legal Studies Research Paper No. 209/2015. *papers.ssrn.com*. Aug. 18, 2015, p 67. Web. Nov. 21, 2021. <https://ssrn.com/abstract=2646447>.
[19] Article 29 Working Party, "Opinion 2/2013 on apps on smart devices", p. 24.
[20] Ibid., p. 24, footnote 44.

In the following sections, this guide focuses on the remaining data protection principles, such as purpose limitation, data minimization, accuracy, storage limitation, security of processing, and accountability, as these are outlined in Article 5 of the GDPR. See figure 4 for a summary of some of the important elements of these principles.

Figure 4: The important elements of the remaining data protection principles

Purpose limitation	• Purposes must be explicit, specific and legitimate. • No further processing for incompatible purposes; if purpose is incompatible, you need new legal ground.
Data minimization	• You must collect only personal data that are strictly necessary to achieve the purposes of processing. • If your app can function without personal data, do not collect them in the first place.
Data accuracy	• Personal data must be accurate and up to date. • If inaccurate, you must take reasonable steps to rectify or erase them.
Storage limitation	• You must not keep personal data in identifiable form for longer than necessary for the specific purpose. • You must have a data retention policy in place.
Integrity and confidentiality	• You must implement appropriate technical and organizational measures to ensure the security of processing. See section 4.6 for what is appropriate.
Accountability	• You as controller are responsible for complying with these principles and demonstrating such compliance in practice (e.g., implement data protection by design and default, carry out DPIAs).

4.2 Purpose limitation

As defined in Article 5 of the GDPR, personal data must be collected for "specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".[21] Following this definition, taken from European Union data protection law, a processing purpose should have the following characteristics. First, the processing should be allowed by law, and not only data protection law, but generally the law applicable to the specific jurisdiction. Essentially, this means personal data cannot be processed for illegal purposes or in a manner that leads to unfair discrimination. In addition, the processing purpose must be

[21] Definition from GDPR, Art. 5(1)(b).

transparent to individual users and clearly articulated, so app providers/developers should be aware of all their processing operations, including whether they are providing access to personal data processed in the app to other actors in the mobile app ecosystem (such as operating system manufacturers, app store providers, third party library providers), and be clear about how such personal data are processed. Moreover, the purpose must be specific in nature; one that is broad or vague, such as improving a user's experience or for marketing or IT-security purposes, will not meet the requirement to be specific.[22]

Moreover, the second aspect of the purpose limitation principle links back to the principle of fair processing, as personal data must not be further processed for purposes that are incompatible with the purposes for which the data were originally collected. Whether a new purpose is compatible with the original purpose will depend on the type of data processed (is it sensitive, for instance), the context of the processing, including the possible consequences for individuals if data are processed for a new purpose, and whether individuals expect or are surprised by the new purpose.[23] For example, an app tracking an individual's physical activity levels by measuring step counts, sleep patterns and dietary habits may process such data to not only show statistics to users about their activity status but also to provide them with reminders in case they miss a day. Arguably, it would be reasonable for individuals to expect this further processing and they may welcome the reminder. But if the app provider/developer offered health insurance services and processed an individual's in-app wellness and health data to set the insurance premium that would be an incompatible further purpose.

When app providers want to use personal data for a new purpose that is incompatible with the original purpose for which they collected the data, they will have to find a new lawful justification and inform individuals of the change, or anonymize the data so it is no longer personal,[xliv] and thus not covered by data protection law.

4.3 Data minimization

Once the processing purposes have been identified, app providers/developers ought to question whether they really need to collect personal data in order to fulfill those purposes. If the app does not need to process personal data in order to work, then such data should not be collected. If the app cannot function without the use of personal data, according to the

[22] Article 29 Data Protection Working Party. "Opinion 03/2013 on purpose limitation." WP203. *europa.eu*. Apr. 2, 2013, p. 16. Web. Nov. 2021. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.
[23] Criteria are from GDPR, Art. 6(4).

GDPR the data collected must be “adequate, relevant and limited to what is necessary”.24 In other words, only the data that are strictly necessary for the specific purposes should be collected and processed, and all other data must be deleted or anonymized. As mobile apps may potentially have access to a broad range of personal data (for example, using various mobile sensors), and employ algorithms to make predictions on future data, providers may consider it useful to collect as much data as possible at the outset of processing just in case it is needed later on, but this would be contrary to the principle of data minimization.xlv Nevertheless, which data are strictly necessary to fulfill a purpose will depend on the circumstances of the processing, and in some cases it may be justified to collect large amounts of data.xlvi Even if that is the case, complying with the principle of data minimization also extends to ensuring that access to the personal data already collected is limited to specific persons acting under the authority of the controller (such as internal employees of the controller) or specific entities (such as third-party service providers) and allowed only when strictly necessary for the provision of a service.xlvii

A relevant example of the practical applicability of data minimization can be found in the context of the design of COVID-19 contact tracing apps. As it became evident these apps could function by collecting only an individual’s proximity data (information exchanged via Bluetooth technology on how close people were to each other and for how long),[xlviii] collecting their exact location or tracking their exact movements across locations and time was not necessary for notifying them of their close contact with someone who had tested positive for COVID-19.[xlix]

In addition, regulators in the European Union also suggested that for the purposes of the apps, it was not necessary to identify individuals, nor was it necessary for the data collected (for example, proximity data) to be processed remotely on a centrally managed server, as the purpose was to notify them, not to use the data for further analysis. As a result, data could be processed locally on an individual user’s device and in an anonymized form,[l] thus the processing would be more privacy-friendly.

Adopting such design measures to comply with data protection principles is an example of how a controller (or a processor, depending on the jurisdiction) may comply with their obligation to implement the principles of data protection by design and by default, both at the time of determining the purposes of processing, and later on, at the time of processing itself. These principles are discussed further in section 6.

---

[24] Definition from GDPR, Art. 5(1)(c).

4.4 Data accuracy

The accuracy principle, as defined in the GDRP, is that personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".[25] Ensuring that personal data are accurate is important, as processing an individual's out-of-date data may lead to identity theft,[li] or other adverse consequences, such as being refused the provision of services or offered services that are not appropriate, for instance, because of inaccurate information about the individual's age or other personal aspect. Individuals also have the right to request the controller rectify inaccurate data or complete any incomplete data; for example, by providing a supplementary statement.[26]

Similarly to the exercise of other data protection rights – the right of access or the right to erasure, for instance, which will be discussed in section 5 – individuals may be able to access their app account and rectify or complete their data themselves in a self-service manner, using the tools and privacy dashboards provided, without having to contact the providers.[lii] Again, these design features can be embedded in the app from the start,[liii] perhaps during the development process, to ensure the controller complies with the data protection principles and with individual rectification rights.

4.5 Storage limitation

The fifth data protection principle refers to the obligation for controllers not to keep personal data in an identifiable form for longer than is necessary for the purposes for which the data are processed. This means that app providers/developers may be required to have a data retention policy in place (that should be included in the information provided in their privacy policy, for instance) that identifies a time frame for keeping personal data and justifies that time frame in relation to the purposes for which the data are processed.[liv] For example, providers may assign different time frames on storing data of active and non-active users, meaning that providers may erase data or even a user's entire account after a specific period of inactivity has passed.[lv] This is logical; as if an individual is no longer using a service (an app), continuing to process their personal data is no longer necessary, unless the controller must continue to do so for some reason, such as to comply with a legal obligation (for example,

[25] Definition from GDPR, Art. 5(1)(d).
[26] See GDPR, Art. 16.

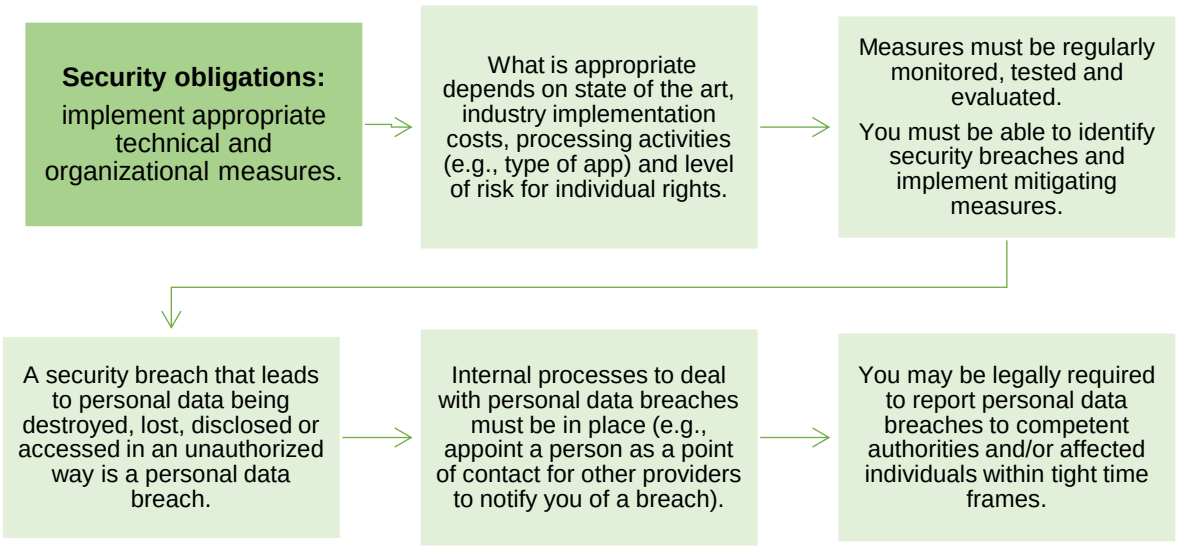
tax or anti-fraud obligations). In practice, app providers/developers may implement storage limitation by default, meaning that according to the nature and type of personal data and the context of processing, specific types of personal data may be automatically erased or anonymized when a specified time has passed.

The principle of storage limitation is also expressed in the individual's right to request erasure of their personal data in certain circumstances, one example being when the data are no longer necessary for the purposes they were collected and processed for.[lvi] In light of this, the provider's data retention policy may include information on the period of time it takes for specific types of data to be erased permanently from their system.[27]

4.6 Security of processing

The obligations regarding the security of processing and dealing with personal data breaches are summarized in figure 5.

Figure 5: Obligations regarding security of processing and dealing with personal data breaches



According to the sixth data protection principle, referred to as the integrity and confidentiality principle, or the security principle, personal data must be processed in a manner that ensures it is protected against "unauthorized or unlawful processing, and against accidental loss,

[27] Kamarinou, D. et al. "Protection of personal data in clouds and rights of individuals." In *Cloud Computing Law,* Millard, C. ed., 2nd edition, p. 280. Oxford University Press, 2021.

destruction or damage, using appropriate technical and organizational measures…".[28] What is considered appropriate will depend on a number of criteria, including the state of the art, implementation costs and the nature, scope, context and purposes of the processing, and the level of risks associated with such processing for an individual's data protection rights.[29] The state of the art refers to the technology available at the time of the processing, the costs of the implementation "…more generally to industry practices [rather] than to specific organizational circumstances".[30] What this means is that regardless of the size of the entity acting as the controller or processor – so regardless of whether an app provider/developer is a single developer or a small or medium-sized enterprise (SME) or a large organization – the obligation to implement appropriate security measures remains the same. The financial and technical resources available to app providers/developers are not a relevant factor unless the specific data protection legislation to which the app provider/developer is subject states otherwise.

In addition, the nature, scope, context and purposes of processing will also be considered when assessing if a technical or organizational measure is appropriate to ensure the security of personal data. For example, processing sensitive data (data revealing racial or ethnic origin, health status or sexual orientation, for instance) may require a higher level of security than processing general personal data, as processing of sensitive data may give rise to a higher level of risk for individual data protection rights. Similarly, the type of app used, and thus the purpose of processing, will have an impact on the level of security that needs to be implemented.

In this context of controllers and processors having to comply with their security obligations, the GDPR provides some examples of what appropriate security measures could be, including:

"… the pseudonymisation and encryption of personal data… the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems… the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident… a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures." [31]

Being able to monitor, detect and respond appropriately to security attacks is important, whether they be routine security incidents or more serious events, when these lead to personal

[28] Definition from GDPR, Art. 5(1)(f).
[29] Definition from GDPR, Art. 32(1).
[30] Kamarinou, D. et al. "Responsibilities of controllers and processors of personal data in clouds." In *Cloud Computing Law,* Millard, C. ed., 2nd edition, p. 318. Oxford University Press, 2021.
[31] See GDPR, Art. 32(1)(a) to (d).

data being lost, disclosed or accessed in an unauthorized way. Some national laws impose an added obligation on controllers to notify the competent data protection authorities (and occasionally individuals) of such personal data breaches within a specified time frame, which may be short (within 72 hours of becoming aware of the breach, for example).[lvii] In complex ecosystems with a number of different entities potentially involved in the same processing, such as the mobile app environment or cloud computing services, a data breach may occur at any level of the supply chain (for example, on the app store provider's platform or the infrastructure of any third-party provider who processes personal data on behalf of the app provider). It may take some time, therefore, for the controller/app provider to become aware of the breach and implement mitigating measures. This is why it may be necessary to embed technical and organizational measures for regular testing and monitoring from the development stage. Further, app providers/developers should include terms on security in their contractual agreements with other providers (whether these act as joint controllers or processors), so the obligations and liabilities of the various parties are explicit and clear. Such terms may include details of the specific security measures that need to be implemented (such as device, system, network security, limits on personnel access, security audits) and who is responsible for notifying whom and within what time frame in the event of a breach.

4.7 Accountability

As discussed, the accountability principle refers to the controller's obligation to comply with all the data protection principles mentioned in this section, and to be able to demonstrate such compliance in practice. Concluding agreements with all the parties involved in the processing of personal data (including other joint controllers and processors), implementing the principles of data protection by design and by default, carrying out data protection impact assessments, appointing independent data protection officers and adhering to industry specific codes of conduct are some of the ways in which controllers can demonstrate they comply with their obligations. Whether processors bear the same obligations will depend on the law of the specific jurisdiction.

The next section provides an overview of the rights individuals may have when their personal data are processed in the mobile app environment. These are important, as the app provider/developer as controller will have to ensure that individuals can exercise their rights effectively. Information about individual rights and ways to exercise them should also be included in the app's privacy policy.

5. INDIVIDUAL DATA PROTECTION RIGHTS

Some of the most important elements of an individual's data protection rights, as outlined in Articles 15 to 17 and 20 to 22 of the GDPR, are summarized in figure 6. The person responsible for facilitating the exercise of those rights is the controller.

Figure 6: Elements of individual data protection rights

Individuals to whom the personal data relate may have a number of data protection rights, including, but not limited to: the right of access to their personal data; the right to rectification and erasure; the right to object to processing and specifically object to processing for direct marketing purposes; the right to data portability; and the right to not be subject to decisions based solely on automated processing or profiling. As personal data may relate to individuals whether or not they are the end-users of a particular app – think of an individual whose photo is shared on a social networking app but who is not a user of the app – app providers should note their data protection obligations, as well as data protection rights, extend to users and nonusers alike; that is, to any individual whose personal data they are processing. In addition,

individuals may also have remedies against the controller or against the decision taken by a competent data protection authority, such as the right to take the controller to court. Moreover, individuals may be able to claim compensation for damages from the controller, or the processor in some jurisdictions, if these damages are caused by the controller or processor infringing their respective obligations under data protection law.

First, the right of access is closely linked to the controller's obligation to provide individuals with all the relevant information about the processing (the principle of transparency). Beyond the information provision, the right of access to personal data may extend to controllers having to provide a copy of all the personal data undergoing processing. This right also covers access to metadata, as these are considered personal data, as well as inferred data produced by app providers when observing and analyzing individual behaviour. According to the Article 29 Working Party, such data may include "…the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations…".[32] As the definition of personal data can be very broad, this should not come as a surprise.

However, an individual's right to receive a copy of their personal data is limited to data that is not personal to others (for example, a document including an individual's personal data may also include personal data of their colleagues) and must not adversely affect any IP rights (for example, revealing proprietary code that is covered by a trade secret). When responding to an access request from an individual, app providers should balance all conflicting rights and decide what personal data to provide without adversely affecting anyone else's data protection, intellectual property, or other rights. It is good practice to document/record the reasons why some personal data may not be provided, as it is the controller's (app provider's) responsibility to demonstrate why and how they have complied with the access request.

Balancing conflicting rights and interests is also at the core of an individual's right to object to processing. This right can be exercised when processing is based on specific lawful grounds, and an individual's objection to processing must be balanced against the controller/app provider's compelling legitimate grounds (such as business, commercial or societal benefits[lviii]) for continuing to process personal data or its obligation to deal with legal claims. For example, a compelling legitimate ground would be processing personal data to maintain appropriate network and system security or to prevent fraud. Additionally, a controller could claim that a legitimate interest would be to process personal data for direct marketing purposes.[lix] However, if an individual objects to their personal data being processed for direct marketing

[32] Article 29 Working Party. "Guidelines on the right to data portability." WP242, rev.01. *ec.europa.eu.* Apr. 15, 2017, p. 10. Web. Nov. 1, 2021. <https://ec.europa.eu/newsroom/article29/items/611233/en>.

purposes, the controller cannot refuse such objection and must stop processing their personal data for such purposes.[lx]

Returning to the right of access, this is an important right, and a prerequisite for exercising all other rights. If an individual knows which personal data the app provider is processing, they can request that these are rectified or completed, and in particular circumstances erased, unless the controller has a legally justifiable reason to continue processing such data. The circumstances under which individuals may request data erasure, or controllers refuse to comply with such erasure, may vary according to jurisdiction. Further, it may be that when presented with an erasure request, they cannot refuse, app providers need to contact all other controllers (app store providers, operating system manufacturers and third-party service providers, among others) with whom they have shared that data and notify them that the individual wants the data erased.[lxi]

Similar to the right of access, individuals may also have a right to data portability, meaning a right to request the controller provides them with a copy of their personal data in a format the GDPR defines as "structured, commonly used and machine-readable", or have such data transmitted directly to another controller.[33] By receiving personal data in such a format, individuals can reuse them. If they request the data be sent to another controller/app provider, they are not locked in a service by a particular provider. This is less broad than the right of access. Individuals have the right to request only the personal data they have provided to the app provider, not all personal data processed about them (not the inferred data produced by the provider, for instance, which is the case under the right of access).

Finally, individuals have a right not to be subject to decisions based solely on automated processing, including profiling that have legal or significant effects on them.[lxii] More specifically, profiling refers to the use of personal data to evaluate certain personal characteristics in order to analyze them and make predictions about people's preferences, location or professional performance, and other types of behaviour.[lxiii] This right refers to situations where a decision is made about an individual without a person being substantially involved in the decision-making process; for example, without an individual critically reviewing the outputs of an automated system (an algorithm). Think of an e-banking app processing an individual's data to decide whether to accept a mortgage application, or a job recruitment app determining whether to show individuals a particular job advertisement or automatically filtering their qualifications to decide whether they should be invited for an interview. In these

[33] Definition from GDPR, Art. 20(1).

situations, the solely automated decision has the potential to affect an individual's rights and obligations (have a legal effect on them), or similarly significantly affect them.

Even if this automated decision-making is allowed under certain circumstances (such as individuals providing their explicit consent, or when the decision is necessary to enter into a contract or under other laws in the jurisdiction), individuals may have a right to have a person intervene in the decision-making process, to have their views taken into account, and the right to appeal against the decision.[34]

For individuals to effectively exercise their data protection rights, controllers/app providers should have appropriate technical and organizational measures in place to support these rights, and be able to respond to an individual's requests. In addition, in their agreements (contracts, for instance) with other controllers and processors, they should have terms dealing with individual rights and the allocation of responsibility, enabling them to respond to individual requests and assist each other in complying.

[34] Provision from GDPR, Art. 22(2) and (3).

6. DEMONSTRATING COMPLIANCE AND CONSEQUENCES OF NONCOMPLIANCE

6.1 Data protection by design and by default

There are advantages (in cost effectiveness and building commercial trust, for instance), in considering data protection from the start of an app development,[lxiv] and technically designing an app in a way that ensures any personal data processing is compliant with data protection law. In general terms, this is what it means to comply with the principles of data protection by design and by default.

More specifically, according to the GDPR rule, implementing data protection by design and by default is an obligation imposed on controllers at the time when they determine the means of processing (deciding how processing will take place, via which software/app store, using which providers, among other things) and also at the time of processing itself (when users actually use the app, for instance). This means controllers must implement appropriate measures throughout the development cycle designed to put in place data protection principles and integrate the safeguards necessary for processing to be compliant with data protection law.[35]

In addition, they must ensure that by default they are processing only personal data necessary for the specific purposes of processing (that they are complying with the data minimization principle, the storage limitation principle and the rules on who may access personal data).[lxv] These principles can be incorporated in the app's default, preconfigured data protection settings. For example, an app's default settings may be designed not to collect unnecessary metadata from uploaded photos, such as the date or location of the image.[36] However, data protection by default is just one part of the design implementation. As implementing data protection by design means that the design measures must take into account all data protection principles, controllers must also ensure individuals can exercise their data protection rights effectively. In that context, the following is suggested:

"… [u]sers should be able to change the pre-configured setting to their needs… When changing a pre-configured "data protection by default" setting, it should be done with the appropriate granularity, thereby preventing that the users' protection is fully lost at once…

[35] Paraphrasing definition from GDPR, 25(1); also see ENISA, "Privacy and data protection", p. 41.
[36] Information Commissioner's Office. "Privacy in mobile apps." *ico.org.uk*. Dec. 2013, p. 8. <https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf>.

After having changed the pre-configured “data protection by default” setting, users should be able to go back to the default setting.”[37]

The appropriate measures will depend on the app provider’s case-by-case risk assessment, which considers the state of the art, cost of implementation (referring to industry standards), context of processing, types and nature of personal data processed and the risks arising from processing that may be of varying likelihood and severity on individual rights.[lxvi] Even though this risk assessment involves the same considerations as when deciding the measures appropriate for the security of personal data, the measures for implementing data protection by design and by default must address the whole range of data protection principles, not just security.

Just as there may be several actors involved in developing and deploying an app in the mobile ecosystem, an app provider as controller may not control the design of all the services/products it may use or incorporate into an app but may still be the ultimate party responsible for compliance with data protection law.

For this reason, in European Union data protection law, other actors (such as processors or producers of products, services or applications), even though not legally required to incorporate these principles, are encouraged to consider the right to data protection when designing and developing their services to ensure these are data protection compliant. Thus, when a controller uses them, they can comply with their data protection obligations.[lxvii] In any case, app providers as controllers should choose only processors that provide sufficient guarantees they have implemented appropriate measures to ensure processing is compliant with data protection law,[lxviii] and include the relevant details in their contractual agreements.

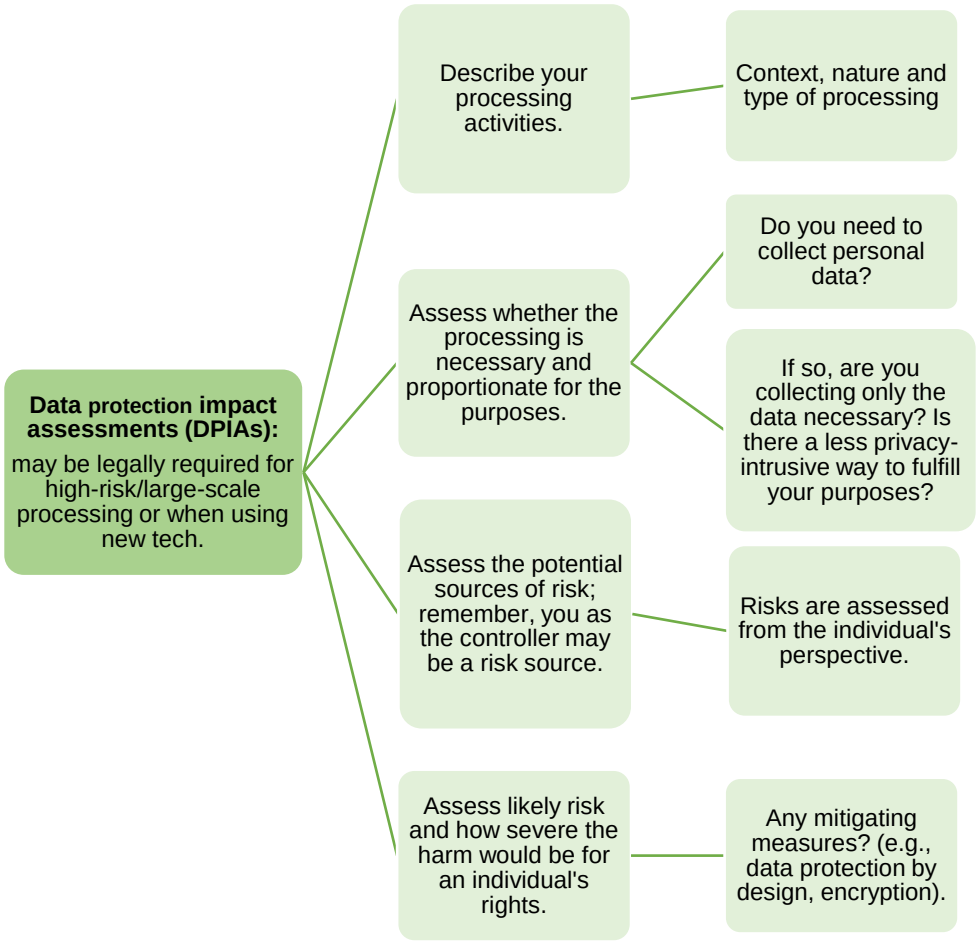
In European Union data protection law, these obligations apply to all entities acting as controllers, irrespective of size, meaning that they apply also to single app providers and SMEs. This point of law may differ between different jurisdictions.

6.2 Data protection impact assessments

See figure 7 for a summary of the basic elements that a data protection impact assessment should include. These are consistent with the requirements of Article 35 of the GDPR.

[37] ENISA, “Privacy and data protection”, p. 51.

Figure 7: Situations when a DPIA may be legally required and subsequent actions



Depending on the context, type and nature of the processing activities, if these are likely to result in a high risk for an individual's rights, controllers may be legally required to carry out a data protection impact assessment (DPIA). Examples of high-risk processing may include automated decision-making, including profiling or processing sensitive data on a large scale; for example, through social networking apps, dating apps, or through wellness apps tracking data revealing an individual's physical and mental health status. In addition, using new technologies to process personal data, combining data from different data sets or processing personal data of vulnerable individuals such as children may also be considered high-risk activities.[lxix]

Even if not a legal requirement, it may be a good idea to carry out a DPIA. It is an exercise in understanding your processing operations, identifying any potential sources of risk and associated harm for individual users, and what can be done to prevent that or mitigate the damage caused, which will demonstrate compliance with data protection law and potentially avoid a high fine. Consistently with Article 35 of the GDPR, a DPIA should contain at least the following:

- Description of processing activities, what types of data you collect and how you use them.
- Assessment of whether such processing is necessary and proportionate for the purposes. Are you complying with the principles of lawful, fair and transparent processing? Are you complying with the principles of data minimization, data quality and storage limitation? Could you achieve your purposes in a way that does not involve the processing of personal data?
- Assessment of the potential sources of risk. This may include an assessment of the vulnerability of your app, or the back-end servers you use, to external security attacks, or how you as the controller may be a risk source, by processing data in an unlawful or unauthorized manner, for instance.[lxx] It is important to note that in a DPIA, the risk is assessed from the perspective of the individuals to whom the data relate.[lxxi]
- Evaluation of the likelihood of risks materializing and causing harm, and how severe such harm may be; for example, following a security breach, an individual's credit card details may become public or their addresses disclosed, together with their geolocation information, and reveal they are not at home, which may make them vulnerable to burglary.[lxxii]
- Assessment of the various measures in place to mitigate such risks and the associated harm to individuals. This could include description and documentation of the security measures implemented or the organizational measures to deal with data breaches (data protection training of employees, and internal procedures to handle a breach, for example), or any other measure implementing data protection by design and by default.

This is a case-by-case assessment, and if any of the essential elements of processing change, these must be reflected in the DPIA (beyond complying with other obligations, such as notifying individuals of the changes). The UK Information Commissioner's Office (ICO) suggests controllers consider publishing their DPIAs to increase transparency and trust.[38]

6.3 Data protection officers

Depending on the jurisdiction, data protection law may require that controllers and processors appoint a data protection officer (DPO) in certain circumstances. Under the GDPR, this is the case when "processing is carried out by a public authority or body"[39] or the controller's or processor's processing activities "…require regular and systematic monitoring of data subjects

[38] ICO, "Privacy in mobile apps", p. 10.
[39] See GDPR, Art. 37(1)(a).

on a large scale; or… consist of processing on a large scale of [sensitive] data… or personal data relating to criminal convictions and offences…".[40] This is because such processing activities may result in high risk to the rights of individuals. Controllers would thus need to draw on a DPO's expert legal knowledge to ensure their processing complies with the law.

A DPO must be able to carry out duties in an independent manner; a controller may appoint a member of staff as DPO but that person must retain their professional independence. Finally, even if controllers and processors are not legally required to appoint a DPO, they may do so voluntarily, as the DPO may be tasked with monitoring compliance with data protection law and providing advice, and cooperating with and acting as the point of contact for data protection competent authorities.[lxxiii]

If controllers and processors appoint a DPO they must publish the officer's contact details (include them in their privacy policy, for instance) and inform the competent authorities. Similar to most data protection obligations, the duty to appoint a DPO is not dependent on the size of the organization acting as the controller or processor, but rather on the nature and risk level of their processing activities, unless data protection law states otherwise.

6.4 Consequences of noncompliance

As mentioned at the outset, designing apps with built-in privacy and data protection may bring competitive advantages in winning consumer trust in the provider's services, but it may also be necessary in order to avoid enforcement actions. Many countries have enacted data protection legislation that empowers competent authorities to conduct investigations regarding data protection violations, and depending on the jurisdiction, impose fines or criminal penalties, which may be high. For example, under the GDPR, depending on the severity of the infringement and other criteria, administrative fines may go up to 20 million euro, "or in the case of an undertaking, up to [4 percent] of the total worldwide annual turnover in the preceding financial year, whichever is higher".[lxxiv] In another example, under Kenya's Data Protection Act, the maximum amount of fines could be "…up to five million shillings, or in the case of an undertaking, up to [1 percent] of its annual turnover of the preceding financial year,

[40] See GDPR, Art. 37(1)(b)(c).

whichever is lower".[41] Individuals may also face a fine of up to three million shillings or prison term of up to 10 years, or both.[42]

Consequently, considering relevant data protection issues from the outset, and complying with data protection obligations and being able to demonstrate such compliance, is essential. The final section will provide a series of key takeaways in the form of practical questions and tips for data management.

[41] Kenya, Kenya Gazette Supplement. "The Data Protection Act, 2019." *kenyalaw.org.* Nov. 11, 2019, sect. 63. <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf>.
[42] Ibid., sect. 73.

7. KEY QUESTIONS

To reiterate, data protection compliance should be considered at the start of the development process, and in any case, before any processing of personal data takes place.

7.1 Baseline questions

Key question	Answer
Does my app need to collect and process personal data in order to work?	• If the answer is no, you must not collect any personal data. • If the answer is yes, you must collect only the personal data strictly necessary for the purposes of processing to comply with the data minimization principle.

Key question	Answer
How do I know which country's data protection law applies to my processing?	• Different countries consider different criteria. • Check if your processing is subject to the law of the country where your organization is established, or where the processing takes place, or where the individuals you offer your services to are located.

Key question	Answer
I am not sure whether the data I am collecting is personal or not. What should I do?	• The UK ICO recommends treating all data as personal from the start.[43] • This is logical, considering the potential for high administrative fines or criminal penalties in case of noncompliance with data protection law.

[43] ICO, "Privacy in mobile apps", p. 4.

Key question	Answer

If I conclude that I am collecting personal data, what should I do next?	• Carry out an internal assessment of your processing operations and how data flows in and out of your app (e.g., which mobile device sensors you are using to collect personal data, which other providers you share personal data with).
	• This assessment may be in a DPIA format, as even in cases where a DPIA is not legally required, it may be good practise to have one (see section 6 for what a DPIA must contain).
	• Identify how you comply with the data protection principles:
	  ○ For example, ensure that analytics data regarding the use of your app are not shared with the app store provider.[44]
	  ○ Identify and document the technical and organizational measures you have implemented to comply with these principles, including to ensure the security of processing, and to deal with personal data breaches.
	• Identify the lawful grounds you rely on to process personal data, and which legal ground corresponds to which purpose of processing.
	• Identify what contractual agreements you must conclude with joint controllers or processors.
	• Depending on whether you transfer personal data outside a specific country, document the contractual measures you are taking to comply with transfer rules.
	• Depending on your processing activities, you may need to appoint a DPO.

[44] qLegal. "A compact guide for start-ups: Embedding privacy by design and default." *Qlegal.qmul.ac.uk.* Web. Nov. 21, 2021. <http://www.qlegal.qmul.ac.uk/media/qlegal/docs/qLegal-Guide-on-Data-Privacy-for-Start-ups.pdf>.

Key question	Answer
I am a single developer/SME. Does data protection law apply to me or to my organization?	• The answer will depend on the specific data protection law applying to the processing of personal data (e.g., the GDPR applies to all controllers and processors, irrespective of organization size[lxxv]).

7.2 Relationship with other actors and agreement obligations

Key question	Answer
I am an app provider but have contracted an app developer to create the app. **What is my role regarding the processing of personal data?**	• If you determine the why and how of processing, you are the controller. • If the app developer is processing personal data on your behalf, they are your processor. • If the app developer creates the app but does not process any personal data, they have merely a technical role as the producer of the app and may not be subject to data protection law.

Key question	Answer
My app is provided to users for free but I generate revenue by incorporating third-party advertising. **What is my role, what is the role of the third-party advertising partner, and what is the relationship between us?**	• If you determined the why and how of the processing, you are the controller. • If the third-party advertising provider collects personal data via your app and processes them for their own advertising purposes, they are also a controller. • It may be that for the specific processing activity, you and the third-party provider act as joint controllers, as you jointly determine the purposes (advertising) and means (the way processing takes place, by accessing personal data through your app) of processing. • It is good practice to have an agreement with your joint controller/s to allocate responsibilities and liabilities.

Key question	Answer
Personal data collected via the app are stored in a cloud service. **What is my relationship with the cloud service provider?**	• As the cloud provider is processing personal data on your behalf, they will be your processor. • It is good practice to have a contractual agreement with your processors to document your instructions for the processing of personal data, detail respective rights and obligations and identify how your processors may assist you to comply with data protection obligations (e.g., processors should be liable for their subprocessor's data protection compliance): ○ In practice, these agreements may be drafted unilaterally by cloud providers.[45] However, you should always read and assess whether their terms comply with data protection law, as you are ultimately responsible for compliance. ○ You should choose processors that guarantee implementing appropriate measures to deal with security and personal data breaches. ○ You should be able to review and regularly audit the processor's compliance, as you should with your own internal compliance.

[45] For more information, see Kamarinou et al., "Responsibilities of controllers and processors", pp. 312–313.

7.3 Obligations towards individuals to whom personal data relates

Key question	Answer
What are my obligations towards individuals to whom the personal data relates?	• Be aware that you may also be processing personal data of individuals who are not users of your app (e.g., collecting emails of other individuals with whom the user wants to share in-app data). • You must comply with the data protection principles and all other obligations imposed on controllers. • You must ensure individuals can exercise their data protection rights effectively. You may provide in-app privacy dashboards where individual users can access, rectify or erase their personal data in a self-service manner.

Key question	Answer

How can I comply with my transparency obligation towards the individuals to whom the data relate?	• You must provide individuals with clear and comprehensive information on your processing activities.
	
	• You may include this information in a document called a privacy policy, which should be available to users before they download and install your app, and also accessible to them while using the app:
	  ○ As processing is context dependent, you should adjust a privacy policy template to reflect your own specific processing activities.
	  ○ Your privacy policy may be multilayered, providing the most important information on the first layer/page and providing links to subpages for more detailed information.
	
	• Information provision is a dynamic process. If the processing activities change, particularly if you are processing personal data for a new purpose, you must inform individuals of the changes as you may need to obtain their consent again (or rely on a different legal ground to process the data for a new purpose).

About the author

Dimitra Kamarinou is a researcher in the Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary University of London, a PhD candidate in the same department and a Greek qualified attorney-at-law. She is the convenor for the Cloud Computing Law module on the Master of Laws (LLM) distance learning programme at Queen Mary. From January 2020 to April 2021, she was also visiting lecturer at King's College London. She has more than 10 years' experience working in law, including for commercial and IP strategy firms, and human rights organizations such as Amnesty International. She has published articles in IT and data protection law, including on issues of machine learning. She holds an LLM in Corporate and Commercial Law from Queen Mary University of London (with merit) and an LLM in Human Rights Law from Birkbeck, University of London (with distinction).

---

[i] Statista. "Mobile app usage – statistics and facts." *statista.com*. Oct. 14, 2021. Web. Oct 29, 2021. <https://www.statista.com/topics/1002/mobile-app-usage/#dossierKeyfigures>.

[ii] Statista. "Most popular app categories worldwide during 3rd quarter 2020, by usage reach." *statista.com*. Sep. 7, 2021. Web. Oct. 29, 2021. <https://www.statista.com/statistics/1252652/top-apps-categories-by-global-usage-reach/>.

[iii] At international level, these principles were introduced by the Organisation for Economic Co-operation and Development, see OECD. "OECD guidelines on the protection of privacy and transborder flows of personal data." *oecd.org*. 1980 <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>, updated in "The OECD privacy framework." *oecd.org.* 2013. <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>; Council of Europe. "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223." *rm.coe.int*. 1981. <https://rm.coe.int/16808ade9d>. All web. Oct. 29, 2021.

[iv] Perez, P.M. and Elphick, E. "WIPO tool on the financing of intellectual property-based mobile apps." *wipo.int*. 2021, pp. 21–22. Web. Nov. 29, 2021. <https://www.wipo.int/export/sites/www/ip-development/en/agenda/pdf/wipo-tool-financing-mobile-apps.pdf>.

[v] For more information see Muyl, C. and Cavalier, M. "What IP practitioners should know about GDPR and personal data protection in Europe." published by Foley Hoag LLP on trademarkandcopyrightlawblog.com. 2018. Web. Dec. 15, 2021. <https://www.trademarkandcopyrightlawblog.com/2018/01/what-ip-practitioners-should-know-about-gdpr-and-personal-data-protection-in-europe/>.

[vi] EUR-Lex. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." *eur-lex.europa.eu*. Apr. 27, 2016. Web. Nov. 2021. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

[vii] Laboris, I. "The impact of the GDPR outside the EU." *lexology.com.* Sep. 17, 2019. <https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f>; for Brazil, see Rudo, H.P. and Reagan, A. "The global landscape of data privacy: important points about new laws in three key jurisdictions." *dlapiper.com.* Sep. 21, 2021. <https://www.dlapiper.com/en/us/insights/publications/2021/09/practical-compliance-the-global-landscape-of-data-privacy-important-points-about-new-laws-in-three/>; for Nigeria, see OneTrust DataGuidance. "Comparing privacy laws: GDPR v Nigeria data protection regulation." *dataguidance.com*. Apr. 14, 2020, p. 5. <https://www.dataguidance.com/sites/default/files/gdpr_v._nigeria.pdf>; for China, see Rouse. "China's New Personal Information Protection Law: must-dos for foreign companies." *lexology.com.* Aug. 31, 2021. <https://www.lexology.com/library/detail.aspx?g=9fae4cd6-0b36-4649-ac11-0c7227294caa>. All web. Nov. 2021.

[viii] European Court of Human Rights. "European Convention on Human Rights." Article 8. *echr.coe.int*. 1950. <https://www.echr.coe.int/documents/convention_eng.pdf >.
[ix] Warren, S. and Brandeis, L. "The right to privacy." *Harvard Law Review*. Vol. IV, No. 5. (1890).
[x] Jurisdictions have different rules on which persons/entities are subject to data protection obligations. For chart comparing GDPR and California Consumer Privacy Act, see Practical Law. "CCPA and GDPR Comparison Chart." *iapp.com*. 2019. Web. Oct. 31, 2021. <https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf>.
[xi] Information Commissioner's Office. "The benefits of data protection laws." *ico.org.uk*. Web. Oct. 31, 2021. <https://ico.org.uk/for-organisations/sme-web-hub/the-benefits-of-data-protection-laws/>.
[xii] GDPR, Art. 83; Deloitte. "Kenya data protection act: quick guide." *deloitte.com*. 2021, slide 3. <https//www2.deloitte.com/content/dam/Deloitte/ke/Documents/risk/Kenya%20Data%20Protection%20Act%20-%20Quick%20Guide%202021.pdf>; OneTrust DataGuidance. "Trinidad and Tobago: data protection overview." *dataguidance.com*. Apr. 2021, sect. 9.1. <https://www.dataguidance.com/notes/trinidad-and-tobago-data-protection-overview>; Linklaters. "Data protected – Philippines." *linklaters.com*. Mar. 2020, sect. on enforcement. <https://www.linklaters.com/en/insights/data-protected/data-protected---philippines>. All web. Nov. 21, 2021.
[xiii] Foitzik, P. "How to leverage your existing privacy program to manage brand reputation risks." *iapp.org.* Apr, 28, 2020. Web. Oct. 31, 2021. <https://iapp.org/news/a/how-to-leverage-your-existing-privacy-program-to-manage-brand-reputation-risks/>.
[xiv] See General Data Protection Regulation. "GDPR." *gdpr-info.eu*. Art. 4(1). <https://gdpr-info.eu>; OneTrust DataGuidance. "Kenya – data protection overview." *dataguidance.com*. Mar. 2021. Web. Nov. 21, 2021. <https://www.dataguidance.com/notes/kenya-data-protection-overview>.; Philippines, National Privacy Commission. "A stronger data privacy law sought in proposed amendments." *privacy.gov.ph*. Jun. 25, 2021. Web. Nov. 21, 2021. <https://www.privacy.gov.ph/2021/06/a-stronger-data-privacy-law-sought-in-proposed-amendments/>.
[xv] For details on processing personal data for anonymization, see Hon, W.K. et al. "The problem of 'personal data' in cloud computing: what information is regulated? The cloud of unknowing, part 1." *International Data Privacy Law.* Vol. 1, issue 4 (2011), pp. 214–217. Also Queen Mary School of Law Legal Studies Research Paper No. 75. *papers.ssrn.com*. Mar. 15, 2011. Web. Nov. 21, 2021. <https://ssrn.com/abstract=1783577>.
[xvi] For example, see GDPR, Recital 26.
[xvii] *Privacy and data protection in mobile applications*. European Union Agency For Network and Information Security (now called European Union Agency for Cybersecurity), Nov. 2017, p. 15. Web. Nov. 21, 2021. <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications>.
[xviii] Ibid.
[xix] Article 29 Working Party. "Opinion 4/2007 on the concept of personal data." *europa.eu*. Jun. 20, 2007, p. 13.
<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.
[xx] For example, GDPR, Art. 3(1) requires the processing of personal data to take place in the context of the activities of an establishment of the controller or the processor in the European Union but Art. 3(2) applies to non-established controllers and processors under different criteria;
Kenya's Data Protection Act of 2019 also applies to organizations not established or resident in Kenya but processing personal data of individuals located in the country, see OneTrust DataGuidance, "Kenya - data protection overview".
[xxi] See GDPR, Arts. 44–49; for Saudi Arabia, see Baker McKenzie. "Saudi Arabia: Personal Data Protection Law enacted." *lexology.com*. Sep. 29, 2021. <https://www.lexology.com/library/detail.aspx?g=3db7fecd-63a2-4684-b16a-8bb64cd12279>. For Russian Federal Law on personal data (No. 152-FZ, dated Jul. 27, 2006), see Linklaters. "Data protected – Russia." *linklaters.com*. Mar. 2020. Web. Nov. 21, 2021. <https://www.linklaters.com/en/insights/data-protected/data-protected---russia>.
[xxii] Kamarinou, D. et al. "Compliance as a service." Queen Mary School of Law Legal Studies Research Paper No. 287/2018. *papers.ssrn.com*. Nov. 14, 2018, pp. 30–31. Web. Nov. 21, 2021. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3284497>.
[xxiii] For example, see GDPR, Art. 8; United States, Federal Trade Commission. "Children's Online Privacy Protection Rule ('COPPA')." Web, Nov. 21, 2021.<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>.

[xxiv] GSMA. "Mobile and privacy: privacy design guidelines for mobile application development." *iapp.org.* Feb. 2012. Web. Nov, 21, 2021. <https://iapp.org/media/pdf/resource_center/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1%20%281%29.pdf>.
[xxv] ENISA, "Privacy and data protection", pp. 12–13.
[xxvi] Terms taken from GDPR. However, other data protection laws use similar terms. For example, the California Privacy Rights Act 2020 uses the term business to describe a role similar to that of a controller, and the term service provider to a role similar to the processor, see IAPP. "The California Privacy Rights Act of 2020." *iapp.org*. <https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/>; Philippines' Data Privacy Act of 2012 refers to personal information controllers and personal information processors, Kenya's Data Protection Act of 2019 to data controller and data processor, and under the Chinese Personal Information Protection Law of 2021, the concept of the personal information handler is similar to the concept of the controller in the GDPR, though there is no formal definition of a processor. See Onetrust DataGuidance. "China – data protection overview." *dataguidance.com*. Nov. 2021. <https://www.dataguidance.com/notes/china-data-protection-overview>. All web. Nov. 21, 2021.
[xxvii] Definition may differ between countries; for example this definition is from GDPR, Art. 4(7).
[xxviii] For example, GDPR, Art. 26.
[xxix] European Data Protection Board. "Guidelines 07/2020 on the concepts of controller and processor in the GDPR." Version 2.0. *edpb.europa.eu.* Jul. 7, 2021, para. 30. Web. Nov, 21, 2021. <https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf>.
[xxx] See GDPR, Recital 78.
[xxxi] For example, see GDPR, Art. 28(3); Philippines, National Privacy Commission. "Implementing rules and regulations of Republic Act No. 10173, known as the 'Data Privacy Act of 2012'." *privacy.gov.ph*. 2016, sect. 44. <https://www.privacy.gov.ph/wp-content/uploads/IRR-of-the-DPA.pdf>.
[xxxii] The accountability principle is one of the fundamental principles of EU data protection law, see GDPR, Article 5(2).
[xxxiii] See GDPR, Art. 30.
[xxxiv] See GDPR. Arts. 35 and 37.
[xxxv] For example, see GDPR, Art. 5; Trinidad and Tobago, Ministry of the Attorney General and Legal Affairs. "Data Protection Act." *rgd.legalaffairs.gov.tt.* 2011, sect. 6. <https://rgd.legalaffairs.gov.tt/laws2/Alphabetical_List/lawspdfs/22.04.pdf>; Philippines, National Privacy Commission. "Implementing rules and regulations of Republic Act No. 10173", sects. 17–19; Kenya, Kenya Gazette Supplement. "The Data Protection Act, 2019." *kenyalaw.org.* Nov. 11, 2019, part IV, sect. 25. <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf>. All web. Nov, 21. 2021.
[xxxvi] For example, the requirements of the EU e-Privacy Directive, Art. 5 and 9, see EUR-Lex. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)." 2002, amended 2009. Web. Nov 21, 2021. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML>.
[xxxvii] These essential elements of consent from definition of consent in GDPR, Art. 4(11).
[xxxviii] This term is used in EU data protection law by the European Data Protection Board, see EDPB. "Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects." *edpb.europa.eu.* Oct. 8, 2019, para. 12. Web. Nov. 21, 2021. <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en>.
[xxxix] For example, see Information Commissioner's Office. "Age appropriate design: a code of practice for online services." *ico.org.uk*. Sep. 2, 2020, p. 6, 36. Web. Nov, 21, 2021. <https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>.
[xl] Information Commissioner's Office. "Privacy in mobile apps." *ico.org.uk*. Dec. 2013, pp. 11–13. Web. Nov. 21, 2021. <https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf>.
[xli] Turton, F. et al. "Privacy in the clouds, revisited: an analysis of the privacy policies of 40 cloud computing services." Queen Mary Law Research Paper No. 354/2021. *papers.ssrn.com*. Apr. 9, 2021, p. 67. Web. Nov. 21, 2021. <https://ssrn.com/abstract=3823424>.
[xlii] ICO, "Privacy in mobile apps", pp. 10–11.

[xliii] Ibid., p. 10.
[xliv] ENISA, "Privacy and data protection", p. 22.
[xlv] Information Commissioner's Office. "Guide to the General Data Protection Regulation (GDPR)." *ico.org.uk*. Jan. 1, 2021, p. 31 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>; and "Big data, artificial intelligence, machine learning and data protection." *ico.org.uk*. 2017, p. 40, 41. Web. Nov. 21, 2021. <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

[xlvi] Kamarinou, D. et al. "Machine learning with personal data." Queen Mary School of Law Legal Studies Research Paper No. 247/2016. *papers.ssrn.com*. Nov. 7, 2016, p. 14, 18. Web. Nov. 21, 2021. https://ssrn.com/abstract=2865811.

[xlvii] Ibid., p. 14.
[xlviii] European Data Protection Board. "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak." *edpb.europa.eu*. Apr. 21, 2020, pp. 13–15. Web. Nov. 21, 2021. <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>.
[xlix] Ibid., p. 11.
[l] Ibid., p. 7, para. 27.
[li] ENISA, "Privacy and data protection", p. 22.
[lii] Turton et al. "Privacy in the clouds, revisited", p. 69.
[liii] ENISA, "Privacy and data protection", p. 11.
[liv] Kamarinou, D. et al. "Protection of personal data in clouds and rights of individuals." In *Cloud Computing Law,* Millard, C. ed., 2nd edition, p. 265. Oxford University Press, 2021.
[lv] Michels, J.D. et al. "Beyond the clouds, part 2: what happens to the files you store in the clouds when you die?" Queen Mary School of Law Legal Studies Research Paper No. 316/2019. *papers.ssrn.com*. May 13, 2019, pp. 11–12. Web. Nov. 21, 2021. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3387398>.
[lvi] For the right to erasure in EU data protection law, see GDPR, Art. 17(1)(a).
[lvii] For example, GDPR, Art. 33 (1); for Philippines, see, Philippines, National Privacy Commission. "Implementing rules and regulations of Republic Act No. 10173", sect. 38. < https://www.privacy.gov.ph/wp-content/uploads/IRR-of-the-DPA.pdf>>; for Kenya, see Kenya Gazette Supplement. "The Data Protection Act, 2019", sect. 43(1).
[lviii] ICO, "Guide to the GDPR", p. 81; also see GDPR, Art. 21(1) for when individuals can object to processing.
[lix] For example, see GDPR, Recital 47.
[lx] For example, see GDPR, Art. 21(2) and (3).
[lxi] This added obligation included in GDPR, Art. 17(2).
[lxii] Definition from GDPR, Art. 22.
[lxiii] Definition loosely from GDPR, Art, 4(4).
[lxiv] ICO, "Privacy in mobile apps", p. 3.
[lxv] See GDPR, Art. 25(2).
[lxvi] See GDPR, Art. 25(1).
[lxvii] See GDPR, Recital 78; European Data Protection Board. "Guidelines 4/2019 on Article 25: data protection by design and by default." Version 2.0. *edpb.europa.eu*. Oct, 20, 2020, pp. 29–30. Web. Nov. 2021. <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>.
[lxviii] See GDPR, Art. 28(1); EDPB, "Guidelines 4/2019 on Article 25", p. 5.
[lxix] For an overview of when a DPIA is required and what a DPIA should include, see GDPR, Art. 35(3) and (7); for details on DPIAs, particularly when an app is addressed at children, see Information Commissioner's Office. "Sample data protection impact assessment: mobile gaming app." *ico.org.uk*. Sep. 9, 2021. Web. Nov. 2021. <https://cy.ico.org.uk/media/for-organisations/childrens-code-hub/additional-resources/sample-data-protection-impact-assessment-mobile-gaming-app-0-0.pdf>.
[lxx] ENISA, "Privacy and data protection", p. 23.
[lxxi] Ibid., pp. 22–23.
[lxxii] For example, see Commission Nationale de l'Informatique et des Libertés (CNIL). "PIA: an overview of the requirements and methodology." *cnil.fr.* <https://www.cnil.fr/sites/default/files/atoms/files/171019_fiche_risque_en_cmjk.pdf>; for useful

guidelines and templates, see CNIL. “Privacy impact assessment.” *cnil.fr.* Web. Nov. 21, 2021. <https://www.cnil.fr/en/privacy-impact-assessment-pia>.

[lxxiii] DPO requirements and duties from GDPR, Arts. 37 and 39.

[lxxiv] See GDPR, Art. 83(5).

[lxxv] The GDPR obligation to keep records of processing activities does not apply to organizations employing fewer than 250 people, but they may still have to comply with the record-keeping obligation if the processing is likely to result in a risk to individual rights, is not occasional or relates to sensitive data. See GDPR, Art. 30(5).