Draft recommendation

On mobile applications

Version submitted for public consultation

until 8 October 2023

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Table of Contents

1. Introduction

Mobile applications are one **of the main means of accessing digital content and services**.

For its users, the multifunction mobile phone (or *smartphone), a*personal terminal by definition, **falls within the private and intimate sphere**. It is essential for everyone to be able to control the data that mobile applications have access to. However, at present, the data processing implemented within applications may be opaque. In particular, information on the existence of data collections and their purposes is often unclear. Similarly, the user may have difficulty understanding the nature of the permissions requested, which complicates the expression of his choices. Finally, multifunction mobile devices carry many sensors more or less known to users (camera, GPS, contact base, accelerometers, etc.) and which can allow applications to access data the collection of which can prove very intrusive.

It is therefore essential that the actors involved in the provision of mobile applications ensure compliance with their data protection obligations and users' rights. However, there are many actors: application developers (some of whom may exchange data), operating system providers, application store managers, software development *kits (SDKs*) related to social networks or technical features, etc.

In practice, data exchanges often take place between these different entities, with sometimes poorly defined responsibility sharing. In particular, the use of SDKs processing personal data (or 'personal data' in the remainder of this document) in a non-compliant manner and the non-compliant use of mobile identifiers have already been subject to formal notice or sanctions by the CNIL[1].

While the data protection principles and obligations are now well known to website operators and are the subject of recommendations from the CNIL, their implementation in the context of mobile applications is sometimes uncertain.

The purpose of this Recommendation is to clarify these rules so that actors in the mobile ecosystem have a good understanding of their obligations and good practices to implement, to facilitate their compliance.

[1] Dec. n° MED 2018-022, 25 June 2018, Dec. n° MED 2018-023, 25 June 2018,Dec. n° MED 2018-043, 8 Oct. 2018, Dec. n° MED-2018-042, 30 Oct. 2018, Dec. n° SAN-2022-025, 29 Dec 2022, Dec. n° SAN-2022-026, 29 Dec 2022.

2. Scope of the recommendation

2.1. Who is this recommendation addressed to?

The purpose of this recommendation is to recall and clarify the applicable law and to guide professionals in the mobile application environment in their compliance with data protection regulations.

It is aimed at professionals operating in the mobile applications sector described below, namely:

- application editors;
- application developers;
- suppliers of software development kits;
- operating system providers;
- app store providers.

This recommendation is addressed in particular to the data protection officers of each of these actors. It is also for the use of all advice on the protection of personal data.

It is primarily intended to help each trader determine his legal qualification within the meaning of the GDPR (responsible or joint controller or processor), in order to better understand his obligations.

The practical obligations and recommendations arising from these qualifications are detailed in the sections dedicated to each actor. However, each actor is invited to refer not only to the recommendations that concern him or her but also to those addressed to his partners, these being likely to affect him incidentally.

The recommendation deals with the processing of personal data of natural persons who use mobile applications.

2.2. What is referred to as a 'mobile application'?

The concept of mobile application refers to application software distributed in the environment of multifunction mobile phones (or *smartphones*) and tablets, i.e. individual and portable terminals, allowing access to the Internet and, most often, to the telephone network, and which can allow the installation and execution of third-party applications within them.

- These applications are most often distributed via broadcast platforms integrated into the terminal by the manufacturers and are run on it in isolation between them (the ' *sandbox*' model). Applications can access a number of system features and data via application programming interfaces (" *application programming interface*") made available for this purpose by the *operating system* (OS).
- This Recommendation covers all types of applications, which may be:
  - 'Native', in the sense that they are developed in the programming language specific to the operating system in which they are run (in practice, Kotlin or Java for Android and Swift or Objective-C for iOS);
  - 'Hybrids', i.e. developed with languages and technologies derived from web programming, and then transformed into application by means of specific tools (such as React or Flutter), in order to maintain over time a uniform code base on all versions of the application;
  - 'Progressive web' (*'PWA*', for ' *Progressive Web App*'), i.e. dynamic web pages which are presented to the user in the form of applications.

How does this Recommendation apply to software environments similar to those of multifunction mobile devices?

In these contexts, if not all recommendations are applicable, stakeholders are invited to take note of them in order to transpose the elements applicable to their situation.

What are these environments?

These are environments allowing applications to be distributed on a mobile operating system suitable for a specific purpose, for example:

- smart speakers, *smart speakers*;
- connected car dashboards;
- sensors and objects connected to the *Internet of Things* or IoT in general;
- individual computing (on Windows, MacOS, Linux, etc.);
- some dedicated environments (e.g.: video games on Steam);
- Etc.

2.3. Who are the players in the mobile applications sector?

Multiple actors are involved in the mobile application ecosystem, which process personal data in different ways. It is mainly the operating system provider, the application store provider, the app editor, the developer and the software development kit editor. Most often, these actors are interdependent.

The operating system provider

What is the role of the operating system provider?

The operating system provider ("OS") shall make available the specially configured operating system installed on the user's mobile terminal, the environment in which the application will subsequently be run.

What is the OS?

The OS is the software brick that defines and supports all authorised interactions between the user and the terminal, but also between third-party mobile applications (those that will be installed afterwards) and the terminal.

Several actors can participate in the construction of an OS as it will be used by the end user.

Thus, a third-party OS provider can choose to use another OS's codebase and then integrate software overlays into its own OS. These software overlays are third-party software components included in the final version of an operating system, as it will be offered to users, adding features that can be used by applications to the OS (e.g.: virtual keyboard applications, voice assistant, etc.). In addition, the mobile device manufacturer may choose to integrate mobile applications that they have not developed themselves and that they have chosen to integrate into their own system (e.g.: office suites, applications of mobile operators). Since these applications are pre-installed, it is not in principle possible for the end user to uninstall them.

This is for example the case for multifunction mobile manufacturers that use an *open source* technical base and integrate third-party software component
s as well as their own applications. This is also the case for mobile phone operators offering for sale multifunction mobile including a batch of pre-installed services.
as well as their own applications. This is also the case for mobile phone operators offering for sale multifunction mobile including a batch of pre-installed services.

The recommendations apply to all actors involved in the provision of this functional brick.

In 2023, some manufacturers (e.g.: Samsung, Oppo, Xiaomi) thus use the AOSP technical base made available by Google (Android Open Source Project: *open source*Android operating system code base) and integrate Google Play Services and/or Google Mobile Services (background services, proprietary applications and application programming interface services produced by Google for Android devices) and their own applications.

What are the processing of personal data involved?
The OS generates and manages identifiers specific to each terminal or user account, which allow the identification of the user for different purposes: technical purposes for the operation of the terminal, advertising tracking, etc. They may be used for the OS provider's own account or transmitted to third parties, including application publishers.

It is also through the software possibilities offered by the operating system provider that the publisher of an application can have access to the various sensors of the mobile terminal (camera, microphone, geolocation of the terminal, accelerometers, etc.) as well as to the data stored on the latter (contact book, photographic gallery, list of installed applications, etc.).

The App Store

What is the role of the app store provider?
The app store provider shall make available the online application distribution platform.

This platform is accessible on the user's terminal from a compatible operating system (e.g. the App Store for a device with the iOS operating system, or the Play Store for a device with the Android operating system).

What is the link between the application store and the operating system?
The app store provider is frequently, but not systematically, the provider of the operating system. However, a specific app store can also be implemented by the terminal manufacturer (Samsung, Huawei, etc.). Finally, especially regarding the Android operating system, many app stores are also available, offered by non-constructors, and can most often be installed as standard applications (F-Droid, Aurora Store, etc.). The app store can lay down the rules applicable to the applications and condition their publication in the store, for example in terms of security measures or user information.

What are the processing of personal data involved?
The establishment of the rules on the publication of applications does not in itself imply the processing of personal data.

On the other hand, the app store may be required to process data for its own purposes, like other mobile applications. In particular, app stores are usually linked to a user account, allowing at least to install app updates.

The application editor

What is the role of the publisher?
The publisher of the application makes it available to users (most often through an app store) to offer its products or services. It also defines the economic model.

What are the processing of personal data involved?
In the majority of cases, the publisher processes personal data when using its application: technical connection data, data provided by the user himself or already present on his terminal, data inferred from his navigation. It can thus be any data necessary for the provision of a good or service through this application (contact, payment, geolocation data, etc.), as well as data related to the operation of the application itself (collection of technical data to ensure the proper functioning of the application, verification of the compatibility of the version of the OS, etc.). The publisher may also transmit the data collected on this occasion to third parties, in particular for the purpose of monetising its audience, through different means specific to the mobile ecosystem (establishment of tracers specific to the mobile environment, making available the user's mobile identifier, etc.).

The application developer

Who is the developer of the application?
The publisher of the application can proceed with the development of its application internally or have it developed by an external developer.

In the first case, publisher and developer merge.

In the second case, the developer develops the application on behalf of the publisher, which can lead him to have access to personal data of the users of the application to carry out the developments requested by the publisher and carry out maintenance operations (pre-production tests, analysis of the data[analysis], reports of errors, etc.).

The developer helps define the architecture and makes the related choices: choice of possible SDKs, hosting arrangements, etc.

What are the processing of personal data involved?

By participating in the development, the developer of the application configures future processing of personal data. By participating in its maintenance, the developer may be involved in all the processing of personal data carried out by the application and sometimes assume some form of liability under the GDPR.

SDK providers

What is the role of the SDK provider?

SDKs (" *Software Development Kits*", or "software development kits") refer to a set of tools used for the development of the application, depending on the operating system used. This practice, which is highly developed in the mobile ecosystem, is due in particular to the fact that SDKs most often facilitate or accelerate the development of software features, allowing the developer to avoid writing the entire code of the application.

What is an SDK concretely?

It is a third-party software brick implanted in the application allowing, like the code written by the developer himself, to carry out different operations. While the SDK can allow operations to be carried out locally on the terminal, in many cases SDKs make it possible to "call" functionalities offered by third-party online services, if necessary by transmitting personal information from the terminal (ID, IP address, configuration, etc.).

The SDK can thus enable certain functionalities to be implemented in the application (e.g.: payment, sharing on social networks, etc.).

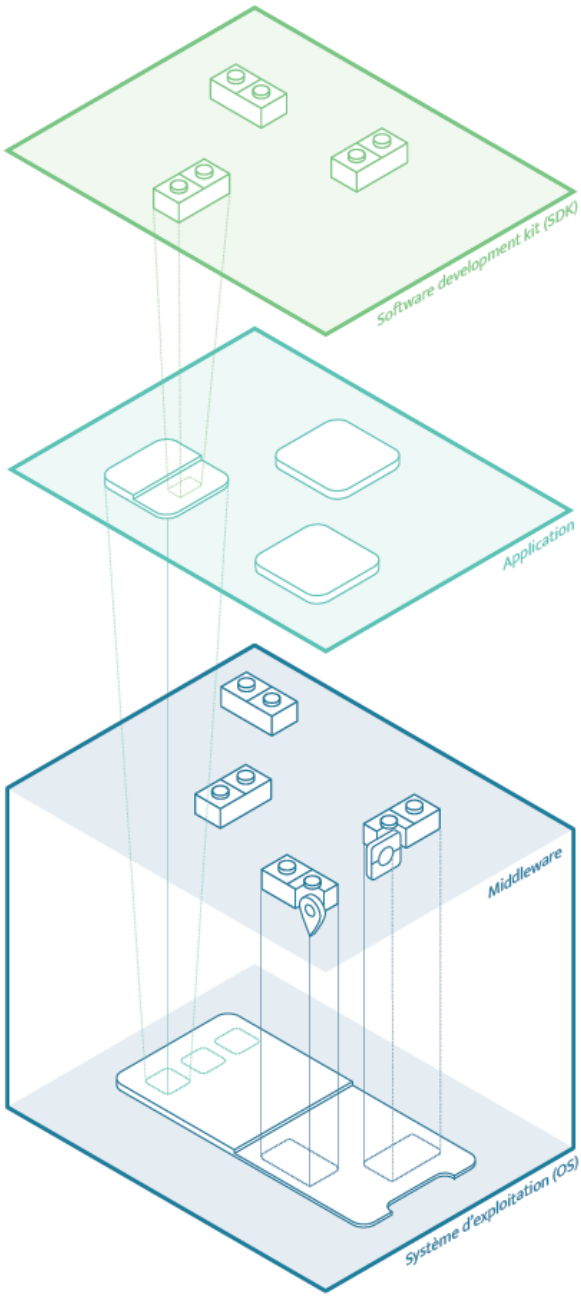
Other SDKs make it possible to make requests for access to the OS, such as the unique advertising identifier associated with the terminal, as well as its geolocation where appropriate (depending on the specificities of the SDK) and thus to trace the user of the application for different purposes: marketing purposes, advertising, etc.

What are the processing of personal data involved?

SDK providers design software bricks that can configure future processing of personal data. They may also be involved in different processing of personal data through these software blocks, depending on the characteristics and purposes of each SDK, and sometimes assume responsibility under the GDPR.

These may include, for example:

- processing consisting of offering certain functionalities through the application, for example image analysis or processing (QR code reading, augmented reality, etc.);
- processing consisting of tracing users for the purpose of analysing the data (analysis)*on*the basis of data provided by the publisher of the application, for the sole benefit of the latter;
- processing carried out by the SDK provider as an advertising intermediary, allowing the publisher of the application to trace its users and to establish profiles for the benefit of third party advertisers or advertisers, to monetise its audience;
- etc.



Éditeurs de SDK

Le **fournisseur de SDK** (***software development kit***) est l'entité qui **met à disposition, un kit de développement logiciel.**

Concrètement, un SDK est un ensemble de fonctions logicielles, de blocs de code, destinés à être intégrés dans des systèmes prédéfinis.

C'est cet aspect qui le distingue du développeur d'application mobile : **un SDK ne peut pas s'exécuter seul, il a besoin d'être intégré dans une application pour fonctionner.** Pour cette raison, un fournisseur de SDK aura de nombreux partenaires : des développeurs et des éditeurs, dont d'applications mobiles.

Éditeurs d'application et développeurs

Le **développeur d'applications** mobiles est la personne, physique ou morale, qui va concrètement **produire le code d'une application mobile.**

L'éditeur d'application mobile est l'entité qui **publie, dans un magasin ou sur sa propre plateforme, une application mobile.**

Il arrive fréquemment qu'il n'y ait pas d'équipe de développement chez l'éditeur. Dans ce cas, l'éditeur fait appel aux services de développeurs, lesquels vont alors produire le code de l'application, pour son compte.

Fournisseur d'OS

Le fournisseur d'OS (*operating system,* système d'exploitation en français), est **l'entité qui met à disposition ce système.**

En pratique, plusieurs acteurs peuvent intervenir dans le développement d'un système d'exploitation : mise à disposition de code sous licence libre ou *open source*, mise à disposition de services logiciels destinés à être intégrés dans des OS, etc.

Le fournisseur d'OS est, lui, responsable de la version finale du système, tel qu'il sera utilisé par les personnes. En pratique, ce terme désigne le plus souvent le constructeur du terminal mobile.

3. Is the application subject to the rules on the protection of personal data?

The recommendations apply to the following operations implemented through an application:

- reading and writing operations on the mobile device as defined by Article 82 of the DataProtection Act, pursuant to theePrivacy Directive, whether or not they relate to personal data.
- Operations constituting the processing of personal data within the meaning of Article 4 of the GDPR.

3.1. Application of the ePrivacy Directive

How do I know if the ePrivacy Directive is applicable?

Article 5 of the **ePrivacy Directive,*transposed*** in Article 82 of the Data Protection Act, is applicable if a reading or writing operation is carried out on the user's terminal through an electronic communication network, namely ' *any action to **access**, **by electronic transmission**, information already stored in his terminal electronic communications equipment, or to **record** information in that equipment*' (Article 82 of the Data Protection Act).

This is in particular the case, when transmitted through a network, of:

- the**use of mobile identifiers (the** unique identifier of the terminal, MAC address, etc.)[2];
- **access to certain information contained in the terminal** (photo gallery, contacts, etc.);
- **access to certain terminal sensors** (camera, microphone, geolocation, etc.);
- etc.

Focus: the role of mobile identifiers

- In the mobile application ecosystem, it is identifiers specific to this environment that allow each user to be tracked in a unique way.
- They may be linked to the mobile device on which the operating system (including the unique advertising identifier) is installed,[3]or to the account of the authenticated user within the operating system environment[4], or be associated with an installation of the application. In the first case, these identifiers allow advertising actors and publishers to uniquely identify the terminal in each application installed on the operating system in order to adapt editorial content and advertising customisation according to the characteristics and behaviors of the user. In the second case, they allow the operating system provider to track users for its own account and purposes.

[2] See point 13 of the CNIL's amending guidelines on *cookies* and other tracers. The use of mobile identifiers may have led to penalties for both app publishers (see Dec. No SAN-2022-026, 29 Dec 2022) and app stores (see Dec. No SAN-2022-025, 29 Dec 2022).

[3]For example, in the Apple environment, it is the ad identifier attached to each terminal (' *Identifier for Advertisers*' or 'IDFA') or the common identifier for the applications of the same publisher (' *Identifier for Vendors*' or ' *IDDFV*'). In the Google environment, the Google advertising ID ("*Advertising ID*" or "AAID") is generated on phones equipped with the Android operating system. Unlike *cookies*, the value of which is set independently for each advertising third party, these identifiers are generated randomly on the first start of the phone and are the same for all third parties. They thus facilitate the linking between these third parties of the data collected about an individual. Coupled with an authenticated environment, they also link this data to an activity on other computer terminals of the user from which the user has also authenticated. This can allow advertising actors to value the data collected about a user in the context of an application by offering targeted advertisements in other applications. This also increases the potential intrusion of this technology into the privacy of*computer users*.

[4] For example, the UDID in the iOS (Apple) environment, for " *Unique Device IDentifier*", which identifies an Apple terminal (iPhone, iPad, etc.).

- These identifiers can thus be passed on to third parties (in particular app publishers, but also advertising intermediaries).
- These identifiers can be unique (i.e. the same identifier is provided to each application that has access to them, making it easier to track interapplications for third parties) or specific to each application editor.

What consequences?

Internet users must be **informed** and give their **consent** prior to these reading and/or writing operations, unless these actions are strictly necessary for the provision of an online communication service expressly requested by the user or have the exclusive purpose of enabling or facilitating communication by electronic means (see Article 82 of the French Data Protection Act and CNIL, deliberations No 2020-091 and No 2020-092 of 17 September 2020[).

3.2. Application of GDPR

Material scope

The **GDPR** applies if the application processes personal data.

If the application processes personal data, **the GDPR will in principle apply to all the processing of personal data carried out by the application.**

Territorial scope

As a reminder and in accordance with Article 3 of the GDPR, this applies:

- The processing of personal data carried out in the context of the activities of actors (processors or processors) established in the territory of the European Union, whether or not the processing takes place in the EU. For example, the GDPR will apply to the processing of personal data carried out within an application published by a company having its sole establishment in the territory of the European Union;
- The processing of personal data of persons within the EU and carried out by actors (processor or processor) who are not established in the EU, where the processing activities are linked to (i) the supply of goods or services to such persons in the EU or (ii) the monitoring of the behaviour of such persons within the EU. Thus, where an application is intended for individuals in the EU and the application processes the data of those same persons, the GDPR will apply to the processing carried out within that application, even if they are carried out by actors located outside the territory of the Union.

3.3. Treatments covered by the domestic exemption

The domestic exemption: what is that?

The GDPR does not apply to the processing of personal data falling exclusively within the scope of the domestic exemption. They must be carried out by a natural person and comply with the conditions laid down in Article 2.2.c and recital 18 of the GDPR. These are, on the one hand, 'personal' activities, which are often specific to the activity of a single individual and carried out in principle in a non-professional setting; on the other hand, 'domestic' activities, which are common to a limited number of persons, in a family or friendly setting.

[). '*Cookies* and other tracers: the CNIL publishes amending guidelines and its recommendation', cnil.fr

Domestic exemption in texts

Article 2.2.c GDPR:

' The [GDPR] *shall not apply to the processing of personal data... carried out by a natural person in the course of a* ***strictly personal or domestic activity****.'*

Recital 18 of the GDPR:

' This Regulation shall not apply to the processing of personal data carried out by a natural person during strictly personal or domestic activities, and therefore unrelated to a professional or commercial activity. Personal or domestic activities could include the exchange of correspondence and the maintenance of an address book, or the use of social networks and online activities that take place in connection with those activities. However, this Regulation shall apply to controllers or processors who provide the means to process personal data for such personal or domestic activities."

What consequences?

Where the domestic exemption applies to processing, **the GDPR does not apply to the natural person carrying out such processing.**

However, the GDPR applies to third parties providing the means of the exempted processing if they can be qualified as controllers or processors within the meaning of the GDPR (recital 18). The domestic exemption then has a limited effect. If, on the other hand, third parties providing the means of processing are not responsible for processing, the GDPR will not apply to the processing of personal data carried out in this context.

In which cases is it considered that the GDPR does not apply to third parties providing the means of the exempted processing?

The CNIL considers that, in principle, if the following two cumulative criteria are met, third parties providing the means of processing under the domestic exemption will not be eligible for any qualification within the meaning of the GDPR (whether as controller or processor) and the GDPR will not be applicable to them by definition:

- the processing is carried out at the initiative, at the discretion and solely on behalf of the person (here the user of the application), i.e. decided and implemented by the latter;
- the processing is carried out under the control of the person, i.e. in complete autonomy, and in a compartmentalised environment, namely without possible intervention of third parties on this data. The third party has provided the means of processing but it no longer acts downstream on the data, does not manipulate it.

In those circumstances, the actor will not determine the purposes and means of the processing actually implemented or act on instructions from another actor determining the purposes and means of the processing. It only provides software to the service of the user.

There are **use cases from the mobile environment respecting these cumulative conditions.**

Thus, for example, the CNIL considered that the GDPR did not apply, under certain conditions, to the publishers of applications providing the means of processing in the following cases:

- Biometric authentication in multifunction mobile devices: this is the case when the processing is carried out on the sole decision of the user, with only local and encrypted storage of his biometric data. Theprocessing is well carried out at the discretion of the person, and the data remain entirely under his control;
- Mobile Health Application: this is the case when the application records and stores the data only locally, without external connection and for exclusively personal purposes, without the application offering features to provide a remote service to its user. In this case, the data is entirely under the control of the user, without possible intervention of third parties on them. The processing is well carried out at the discretion of the person, who uses the application only in the context of personal use.

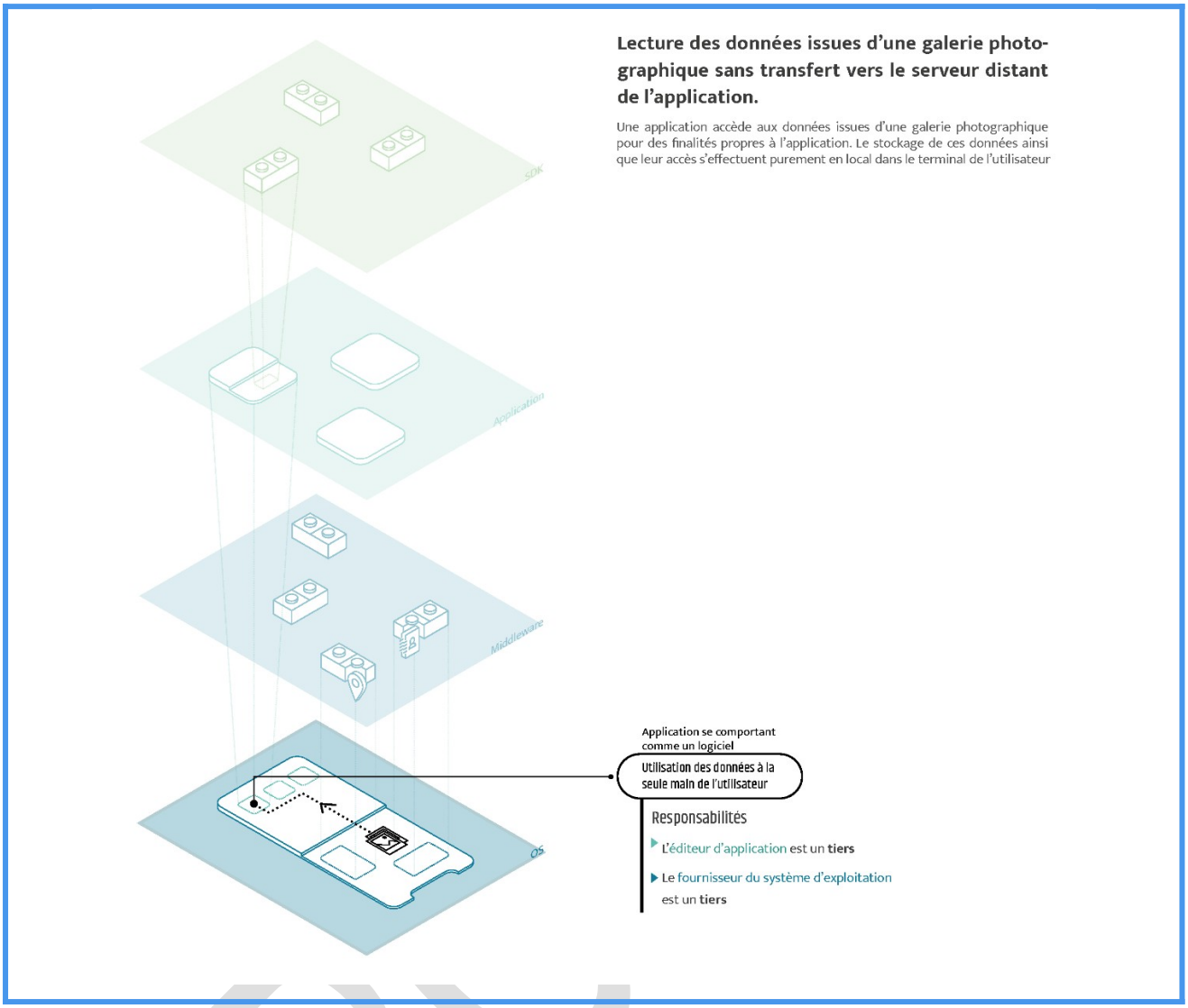
The same reasoning could apply to app publishers providing the means of processing in the following cases:

- Data sharing in *peer-to-peer mode,*i.e. without storage or transit via a centralised server;
- Applications operating as simple software made available to the user (e.g.: keyboard with scalable configuration (“learning”) local without federation, features involving interaction between the user and pre-recorded data statically in the application).

In practice, an application that operates without any intervention or data transmission from its provider has a high probability of being able to fall under the domestic exemption. An application that could continue to work normally despite the disappearance of its editor is particularly likely to meet these criteria.

Example: read data from a photo gallery without transfer to the application’s remote server

An application accesses data from a photographic gallery for application-specific purposes (for example, to allow the photo to be retouched). This data is stored and accessed only within the user’s terminal, without any information being shared with the servers of the application publisher or with those of the operating system provider. Neither the publisher nor the operating system provider can intervene in any way on this data.
In this case, the application functions as a simple software made available to the user. The publisher and the provider of the operating system must then be regarded as mere third parties, insofar as they do not determine the purposes or means of the processing of the data.



The CNIL strongly encourages the provision of mobile applications based on treatments carried out entirely at the initiative and under the control of the person under the conditions defined above: these applications and the resulting treatments thus fall within the scope of the domestic exemption and guarantee respect for privacy by design.

However, the CNIL makes two complementary recommendations for these domestic treatments:

- since applications covered by the domestic exemption are under the exclusive control of users, the CNIL urges them to ensure the safety of their applications: among other things, they are recommended to keep the versions of their applications up to date and not to use an application for which software vulnerabilities are known. As a good practice, in the latter case, the CNIL recommends that the publisher of the application indicate whether it should no longer be used, or that it be delisted from the application store;
- the publishers and designers of these applications, although not covered by the GDPR for the implementation of the processing operations and are therefore not subject to security obligations, should design them in accordance with the principles of minimisation and data security of the GDPR in order to limit the risks that users run in the event of compromise.

What qualification of the application publisher providing the means of domestic processing if the GDPR is applicable to it?

As a reminder, the user of the application complying with the conditions of the domestic exemption cannot be qualified as a controller thus exempted.

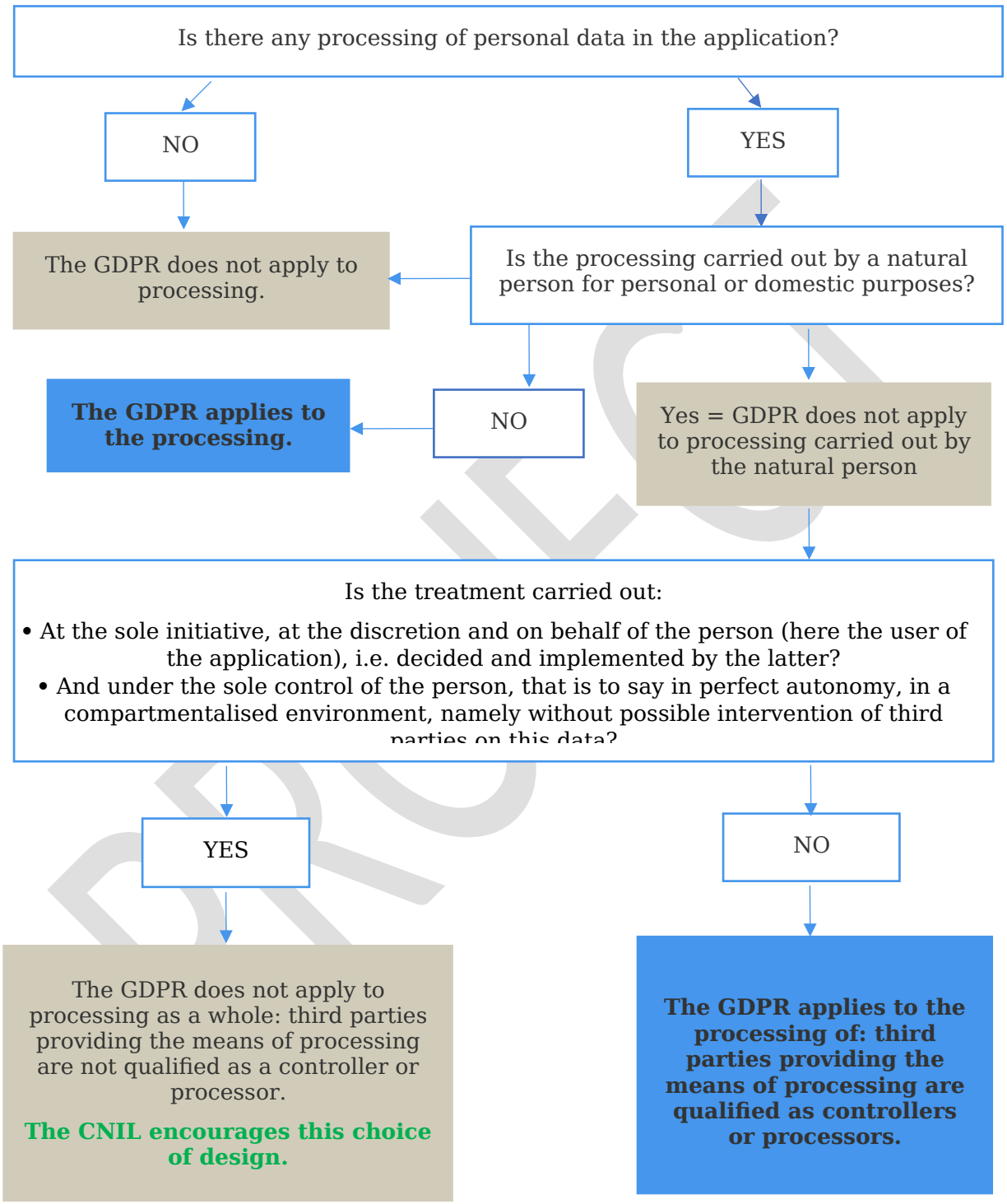
On the other hand, the GDPR applies to the publisher of the application, provider of the means of processing, where the latter does not comply with the cumulative conditions specified above, in which case it must be classified as a controller.

Example: creation of a shared album of family photos within a photo gallery application

In this case, the GDPR does not apply to the creator of the photo album because this processing is carried out by a natural person as part of a strictly domestic activity, in order to share family photos with family members.

On the other hand, the editor of the photo gallery application must be qualified as the controller from the moment the album is stored in third party servers (the app editor or others) to be shared among other users.

To remember: questions to ask as a developer, publisher or provider of SDK to determine whether the GDPR applies to the treatments implemented in the application



References

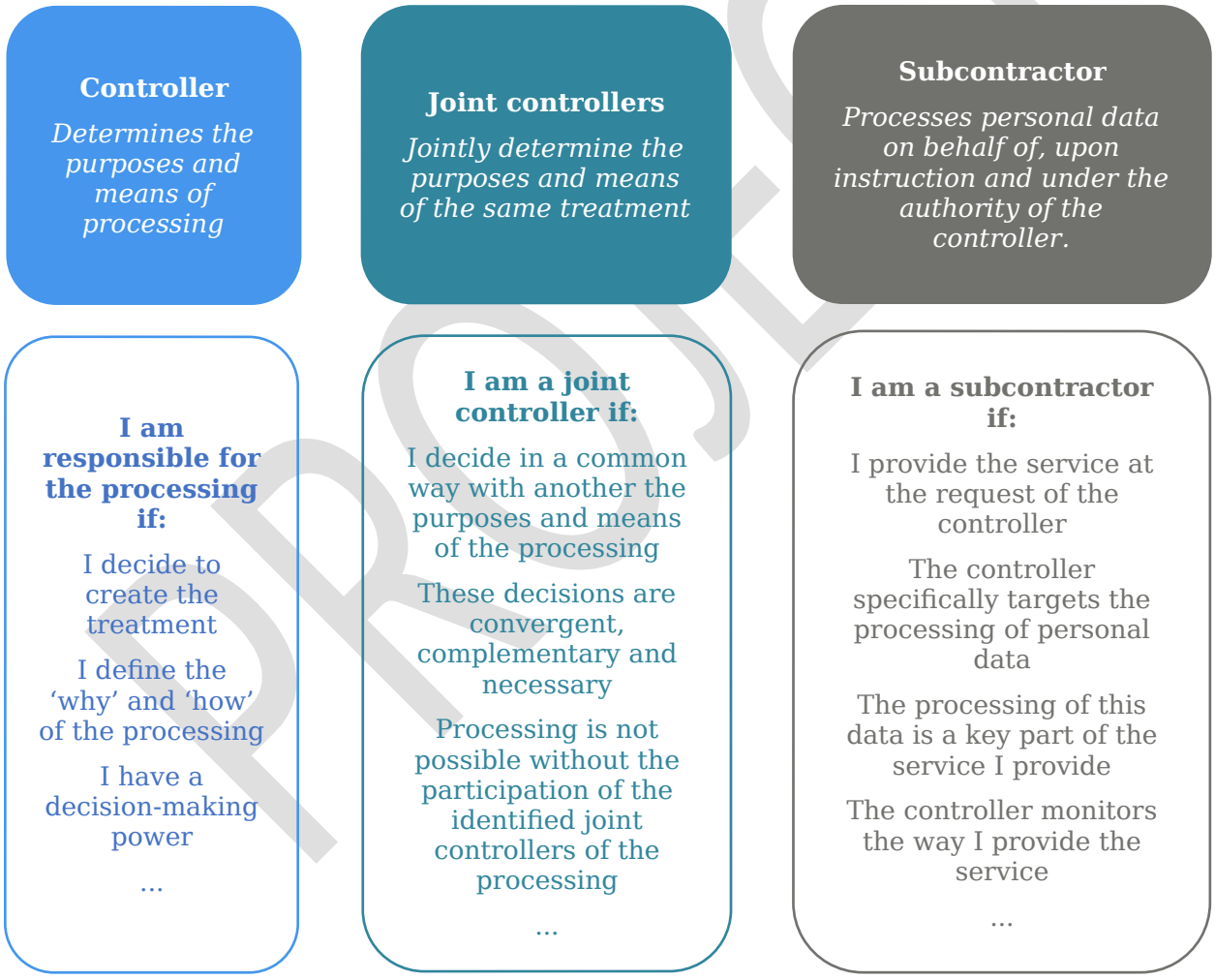
- Article 2 GDPR
- Article 4 GDPR
- Article 82 of the Data Protection Act

4. What are the roles of each actor in the use of the application?

4.1. Why is it important to determine the role of everyone within the meaning of the GDPR?

Not all actors involved in the mobile application environment have the same role in the processing of their users' personal data. If the GDPR applies to them, they may fall into one of the following three categories:

- Controller[5];
- Joint controller;
- Subcontractor[6].



[5] Natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing (Article 4.7 GDPR).
[6] Natural or legal person,' public authority, department or other body that processes personal data on behalf of the controller (Article 4.8 GDPR).

The dividing line between these three qualifications can sometimes be tricky, since a multitude of actors are involved in the development and operation of mobile applications and the way in which personal data is processed is unique for each application.

It should also be stressed that other actors may be contractually involved in the design, development, distribution and operation of a mobile application, without having any of these three qualifications.

The question of the qualification of each actor arises for each processing of personal data carried out within an application.

In accordance with the principle of *accountability* laid down by the GDPR, it is up to each actor to determine its own qualification in the light of its actual role; players cannot choose as an opportunity the qualification they prefer: they must be able to argue and explain the qualification chosen, specifying the reasons which led to the choice of that qualification, and in particular: who decided to create the processing? who defined its purpose? what personal data are collected? what are the retention periods? what are the security measures put in place? etc. Stakeholders must demonstrate that a thorough reflection has been carried out to determine the qualification to be used, from the point of view of the criteria differentiating the controller, the joint controller and the processor. Reflection on the qualification of actors can be formalised in different types of media such as the Data Protection Impact Assessment.

4.2. Determine the qualifications of each actor

Point of attention

The qualification of the actors must be carried out on a case-by-case basis. The examples below do not prejudge the qualifications that could be used in practice, taking into account the specificities of the particular situations and the modes of operation faced by the various actors.

The supervisory authorities are not bound by the qualifications chosen by the parties, in particular within the contracts; a requalification, assessed in the light of the justifications provided, is therefore always possible.

Qualifications of the publisher

In which cases can the publisher of the application be responsible for processing?

Since it does not merely provide the software but participates in its operation (for example, if this operation involves communications between the user's terminal and the publisher's servers), the publisher of the application is, in principle, responsible for the processing of the user's personal data carried out in the application because he has determined its purposes and means, i.e. the purpose and the way of achieving them (nature of the data collected within the application, duration of data retention, security requirements, etc.).

In particular, he may be **responsible for**:

- **processing of personal data carried out in connection with the use of the services offered through the application, for example:**
  - data resulting from the management of the user's account (surname, first name, email address, telephone number, etc.);
  - the data necessary for the use of the services offered within the application (delivery address, bank details, discount card number, etc.);
- **the reading and/or writing operations that it carries out on its own behalf, as well as the processing of personal data resulting therefrom.** These include:
  - reading mobile identifiers for various purposes, for example:
    - reading the mobile's unique advertising identifier in order to enable third-party advertisers to track the user's behaviour in the application;

        - read by the provider of an app store (as an application editor) the user account identifier to personalise the suggestions within the app store;
        - read by the operating system provider (as a system application editor) the user's account identifier to track its activity to improve its functionality;
        - etc.
    - access to the various sensors of the mobile terminal (camera, geolocation, etc.) when the data is transmitted through a network for various purposes, for example:
        - reading the user's geolocation to facilitate navigation within a route calculation application;
        - use of the camera sensor by an application to scan a QR code;
        - etc.
    - access to data stored on the mobile device (contacts, photo gallery, file explorer, etc.) for various purposes, for example:
        - access to files stored by the user to provide backup functionality;
        - access to the user's photo gallery to upload a profile picture;
        - access to a contact book for the discovery of contacts in the context of the use of instant messaging;
        - etc.
- **reading and/or writing operations carried out by third parties**[7] **(jointly with these third parties if they jointly define the purposes and means of processing)**. For example:
    - reading the unique advertising identifier by a third party SDK used by the application for the purpose of profiling users on behalf of the publisher: the publisher of the application is responsible for the processing of the transaction consisting of the reading of the advertising identifier (possibly jointly with the SDK provider);
    - reading a technical identifier by a third party SDK through the application on behalf of the third party to produce statistics for the purposes of improving its service: the publisher is jointly responsible for processing only in respect of the operation consisting of the reading of the technical identifier;
    - etc.
- reading and/or writing**operations carried out by third parties on behalf of the publisher as well as the resulting processing operations which are also carried out by these third parties on behalf of the publisher.** For example:
    - the publisher of the application is responsible for the operation carried out by the third-party SDK provider of reading the unique advertising identifier as well as the user's ad profiling processing carried out by the SDK provider on behalf of the publisher on the basis of that transaction;
    - etc.

On the other hand, the publisher is not responsible for the processing carried out by third parties on their own account on personal data derived from reading and/or writing operations that they carry out through the application. Once the processing uses the data collected through the application, through a collection operation for which the

[7] In the web environment, the responsibility for processing the publisher of a website was thus retained in relation to the reading/writing operations carried out by third parties in a decision 'Editions Croque Futur', No 412589 issued by the Conseil d'État on 6 June 2018, in which the Conseil d'État considers that the publisher of a site which authorises the deposit and use of third-party *cookies* must be regarded as controller.
Similarly, in a deliberation n° SAN-2021-013 of 27 July 2021, the CNIL considered that the publisher of the site had some responsibility (an obligation of means) for the collection of consent on third-party *cookies*. Thus, the fact that *cookies* come from partners does not relieve the publisher of the site of its own responsibility to the extent that it has control over its site and its servers.

publisher is co-responsible, the third party must duly inform and obtain the publisher's consent before recovering the data to implement such processing on its own account. For example:

- reading a technical identifier through the application on behalf of the third party to produce statistics for the purposes of improving its service: the publisher is not responsible for the subsequent statistical processing carried out by the third party on the basis of that operation;
- reading the unique advertising identifier of the application on behalf of the third party for the purpose of crossing data with those from other applications to achieve its own advertising purposes: the publisher is not responsible for the processing of data crossover carried out by the third party on the basis of this operation;
- etc.

To go further

The CNIL has published a fact sheet on the re-use by the processor of the data entrusted by the controller[8]. This is applicable to the processing of personal data carried out by third parties on their own behalf through a mobile application.

Developer qualification

The publisher may, depending on the case, have its application developed by an external developer. The question then arises of the qualification of the developer if the GDPR is applicable to him.

Note: when the publisher develops its application internally, editor and developer merge and have the same responsibilities.

In which cases does the developer of the application not assume any form of liability under the GDPR?

If the developer merely provides the publisher with the code of the application that he wishes to offer to the public, but then no longer has any role in its operation or control of the personal data processed by the application, he is neither controller nor processor within the meaning of the GDPR.

In practice, however, the developer's role is essential for the application to be designed in a way that respects GDPR principles. Furthermore, while the responsibility for carrying out the data protection impact assessment lies legally with the controller, the security of the application is in practice based on the choices of the processor. The CNIL therefore recommends, in this configuration:

- whereas the contract between the developer and the publisher requires the developer to design an application allowing the data processed to be processed in accordance with the GDPR and in a logic of*privacy by design*;
- that the editor be associated with the structuring choices, including security, throughout the design of the application.

Finally, it is recalled that providing an application whose operation would by itself disregard the GDPR may give rise to the developer's civil liability vis-à-vis the publisher[9].

In which cases can the developer of the application be subcontracted?

The developer can often be qualified as a **processor** if he processes personal data on behalf of the publisher, acting as the controller. This may be the case, for example, where:

- the developer shall implement the data processing and storage infrastructure relating to the mobile application;
- the developer carries out operations on data hosted on the application's server for the purposes of maintenance or outsourcing of the application;

[8] 'Subcontractors: the re-use of data entrusted by a controller', cnil.fr

[9] The contract between the publisher of the application and its developer may, in particular, be invalid if the non-compliance with the obligations of the other party under the GDPR constitutes an error as to the essential qualities of the subject-matter of the contract (see, to that effect, CA Grenoble, 12 Jan. 2023, No 21/03701, in the case of website design).

- etc.

In which cases can the developer of the application be responsible for the processing?

By way of exception, the developer may be qualified as a separate **controller** of the publisher if he processes data on his own behalf, for purposes he defines.

This may be the case, for example, where:

- the developer processes personal data from the application for the purposes of improving the security of the other applications it develops;
- the developer processes personal data from the application to produce statistics for the purposes of improving its own services;
- the developer crosses data from different applications in order to offer new services;
- etc.

When considering using data collected through the application on his own behalf, the developer is obliged to inform the publisher of the application of the purposes of this collection and obtain his prior consent before recovering the data to implement such processing on his own account.

To go further

The CNIL has published a fact sheet on the re-use by the processor of the data entrusted by the controller[10]. This is applicable to the processing of personal data carried out by third parties on their own behalf through a mobile application.

Qualification of SDK provider

The publisher may, as appropriate, use SDKs when developing its application (see paragraph on SDK providers above).

In some cases, the publisher may use it on its own initiative, when it itself develops its application or when it expressly instructs its developer to include an SDK due to a commercial agreement.

In other cases, it does not decide directly to use it, when the development of the application and the choice of SDK is carried out by an external developer.

In practice, data exchanges often take place between these different actors. The question then arises of the qualification of the SDK when the latter processes personal data, it being clarified that the GDPR does not apply to SDK which does not process any personal data from the application to carry out the developments (e.g.: this may be the case in particular when the SDK provided does not process any personal data, and in particular does not process the IP address of the user of the application).

In which cases can the SDK provider be a subcontractor?

The SDK provider may be qualified as a processor when processing personal data on behalf of the publisher responsible for the processing.

This may be the case, for example, where:

- the SDK performs reading and/or writing operations solely on behalf of the publisher;
- the SDK allows the use of a payment service within the application;
- the SDK analyses a user's behaviour on the mobile application for the purpose of profiling it for advertising purposes on behalf of the publisher, by reading the unique advertising identifier of the terminal;
- the SDK analyses the geolocation of the user of a mobile application in order to profile it on behalf of the publisher.

In the event that the development of the application is ensured by a processor of personal data, the provider of the SDK set up in the application by the external developer would be considered as a subcontractor of the original subcontractor.

[10] 'Subcontractors: the re-use of data entrusted by a controller', cnil.fr

In which cases can the SDK provider be responsible for the processing?

The SDK provider may be responsible for certain processing of personal data carried out in the application, if it determines its purposes and means, i.e. the purpose and the manner in which it is carried out.

In particular, he may be responsible for:

- **reading and/or writing operations that he performs (jointly with the publisher who allows this collection).** These may include, for example:
  - the reading of the unique advertising identifier through the application for the purpose of profiling users;
  - the reading of a technical identifier of the user's terminal through the application to produce statistics for the purpose of improving the service;
  - etc.
- **processing of personal data resulting from these operations, when they are carried out on his own account with the prior consent of the publisher.** The SDK provider is obliged to ensure the correct information of the publisher of the application, responsible for the initial processing, before carrying out such processing on its own account, in particular in the contractual elements with it. These may include, for example:
  - the statistical processing which it carries out on the use of its service carried out by monitoring the users enabled by reading the technical identifier of their terminals, for the purpose of improving its service;
  - etc.

To go further

The CNIL has published a fact sheet on the re-use by the processor of the data entrusted by the controller.

This is applicable to the processing of personal data carried out by third parties on their own behalf through a mobile application.

Qualification of the operating system provider

In which cases can the operating system provider be responsible for the processing?

The operating system provider may be considered responsible for the processing of the terminal, which may constitute processing of personal data, for certain purposes of securing or operating the OS (e.g.: search for OS updates, telemetry, service improvement, fraud detection), as long as it determines its means and purposes.

These processing operations are, for a large part, independent of the applications that may be executed within the operating system, but some are related to them, in particular because they provide applications with information and identifiers, some of which are personal data about the user.

Certain situations need to be analysed on a case-by-case basis to determine the qualification of the operating system provider, according to the parameters and specificities of each environment, including:

- the operation of creating a mobile identifier locally;
- the provision of a mobile identifier to a third party, in particular an application publisher;
- the provision of other information on the user's terminal to third parties, in particular application publishers. This is the case in particular with the provision of the location, the contact book or the photo gallery.

These analyses must take into account each specific environment:

- in the case of iOS, all other actors (publishers, developers, SDKs) can only contact one entity, Apple, regarding these issues. In addition, there is no other app store provider than the App Store on iOS and iPadOS.

- in the case of Android, on the other hand, third parties to the OS (publishers, developers, SDKs) can contact different entities[11].
- thus, these different entities are likely to share responsibilities based on the re-use of data that is made, in particular between Google, which may then have to **reuse data on its own account, and the manufacturers.**

In any event, and even where they are limited to providing technical tools without processing themselves, OS providers determine to some extent, through their technical choices, the way in which the processing of personal data is carried out by application publishers. As such, OS providers are covered by certain recommendations (see Part 8 of these recommendations: 'OS provider-specific recommendations'), irrespective of their responsibility within the meaning of the GDPR, with regard to the configurations they determine (collection of different permissions, access to APIs, etc.). These recommendations applicable to OSs may constitute legal obligations in the event that the publisher of the OS is classified as a controller.

Qualification of the application store

What role for the application store setting the rules for the publication of applications?

The app store apprehended as an actor laying down rules on the publication of applications within the app store does not therefore have a qualification within the meaning of the GDPR. Indeed, if it can, to some extent, influence the publisher and/or the developer on the compliance of applications with the GDPR (e.g. by defining rules for the submission of permission requests to the user), this circumstance does not affect his responsibilities under the GDPR because he does not process personal data on that occasion.

And when the app store provider acts as the store's publisher, as a mobile app?

On the other hand, the store's publisher, perceived as an app editor, will be subject to the same qualifications and obligations as for any app publisher. Thus, when the application store processes personal data for its own purposes (e.g.: processing of developer data in the context of application review processes prior to publication, processing of a possible unique identifier for its own purposes, processing of specific information such as the list of applications installed by the user and their status), it may be qualified as controller as long as it defines its means and purposes.

Examples

Read and process a mobile ID by an SDK on behalf of the publisher and on its own account

An application editor uses the services of an SDK provider to facilitate the development of its application. This one introduces an SDK into the application whose functionality is to access the unique advertising ID of the mobile in order to be able to track the behavior of the user in the application. If the user has given his consent, the SDK queries the operating system to access the mobile advertising ID. The SDK measures thanks to the tracking allowed by the ID the interactions between the user and the application and performs analyses on behalf of the publisher of the application in order to allow it to know its audience and thus monetise the advertising spaces present in the application to advertisers. The data collected by the SDK allow its provider to pursue its own purposes, namely the improvement of its user profiling

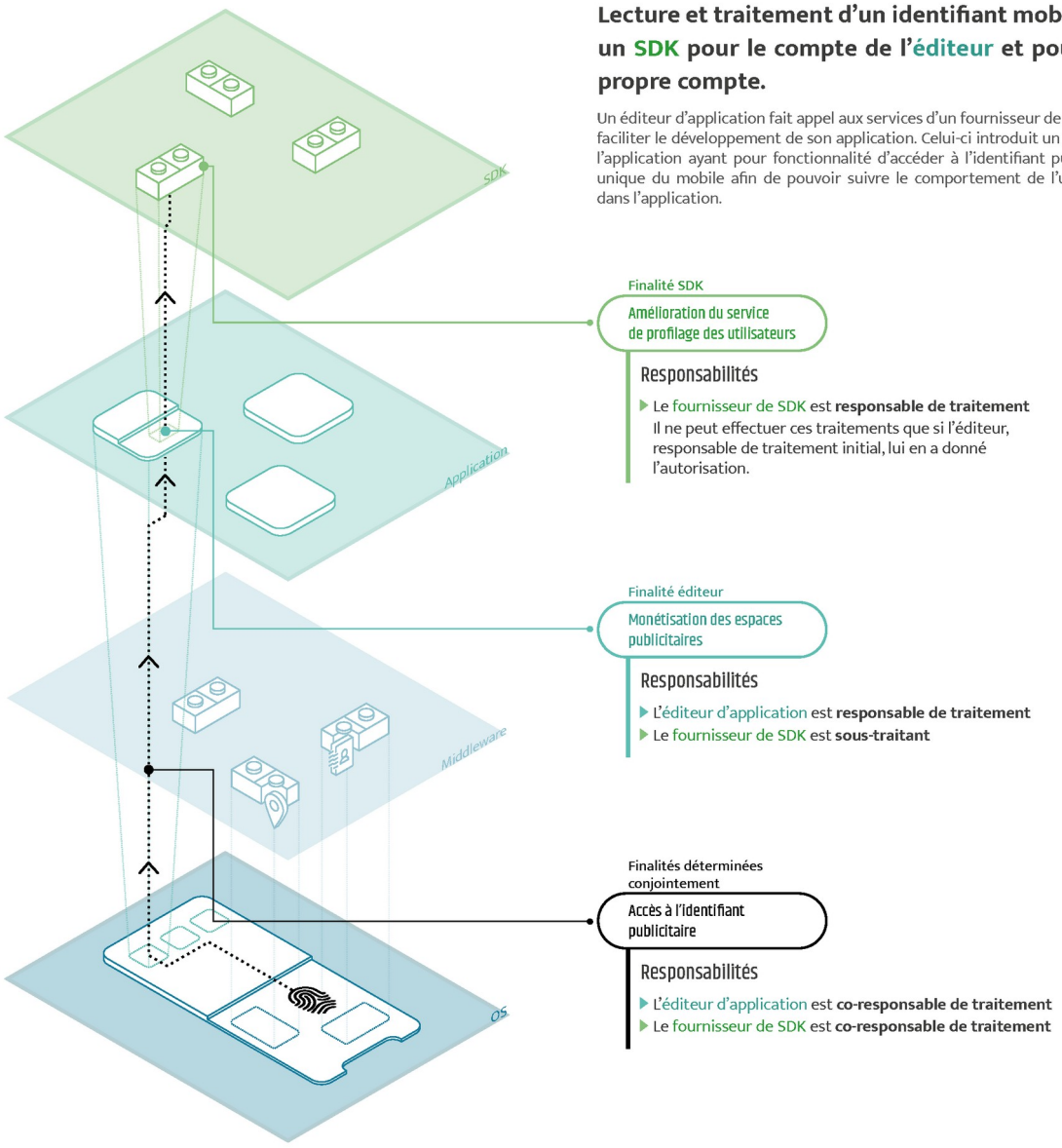
[11] Thus, by way of example, at the date of adoption of this Recommendation, an Android operating system will consist of:

- AOSP (*Android Open Source Project*: provision by Google of the code base of the Android operating system as *open source)*,the Google Play Services and GMS (software suite published by Google allowing access to other features, including Google services (Chrome, Youtube, Gmail, etc.) for Google terminals; or
- AOSP, Google Play Services, GMS and a builder suite (somemultifunction mobile manufacturers are developing their own suite of applications to integrate the operating system of their devices) for certain terminals (Samsung, Oppo, Nokia, Blackberry, OnePlus, Motorola, Xiaomi, etc.); or
- AOSP and a software suite build for others (Huawei, Amazon, Murena, Fairphone, etc.), without the use of Google Play Services or GMS.

service for all its customers.

In that case:

- the publisher and the provider of SDKs are jointly responsible for processing the inclusion within the application of an SDK whose function is to access the advertising identifier (which constitutes a reading and/or writing operation within the meaning ofArticle 82 of the Data Protection Act) by the SDK provider because they jointly participate in the determination of the purposes and means of the processing;
- as regards the processing carried out by the SDK provider on the personal data collected through access to this advertising identifier on behalf of the publisher (monetisation of advertising spaces in the application), the publisher is responsible for the processing and the provider of SDK its processor;
- the SDK provider may also process the personal data collected through access to this advertising identifier for its own purposes, only if the publisher, responsible for the initial processing, has been properly informed and integrates the SDK with knowledge of the existence of such processing (e.g. via contractual elements). In this case, the



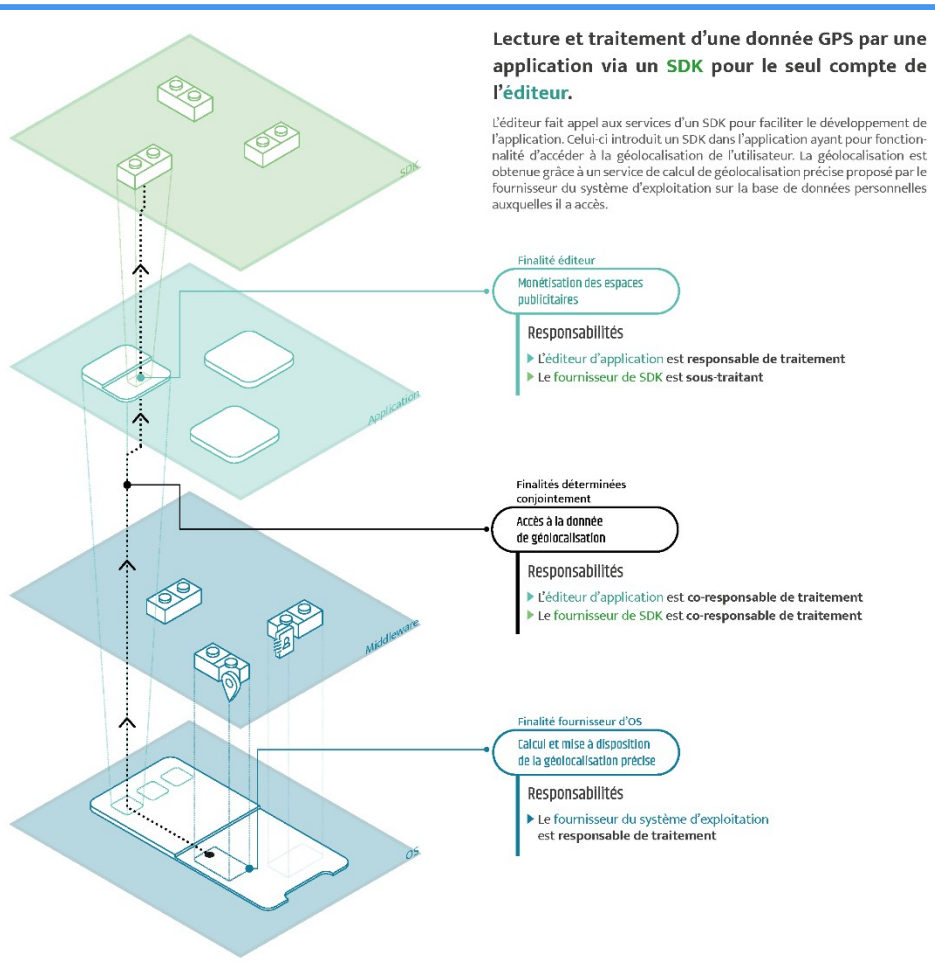
SDK provider is responsible for the processing.

Read and process GPS data by an application via an SDK for the publisher's account alone

The publisher uses the services of an SDK provider to facilitate the development of the application. This SDK has the functionality of accessing the geolocation of the user. This information is obtained through a precise geolocation calculation service offered by the operating system provider on the basis of personal data to which it has access (IP address, lists of Wi-Fi hotspots and Bluetooth identifiers around the terminal). Access to geolocation is for the benefit of both the user and the publisher. Indeed, this allows the user to benefit from certain features of the application. The SDK also uses this geolocation information to carry out analyses on behalf of the publisher of the application in order to allow it to know its audience and thus monetise the advertising spaces present in the application to advertisers.

In that case:

- the publisher and the provider of SDKs are jointly responsible for processing the inclusion within the application of an SDK whose function is to access the geolocation data (which constitutes a reading and/or writing operation within the meaning of Article 82 of the Data Protection Act), because they jointly participate in the determination of the purposes and means of the processing;
- as regards the processing carried out by the SDK provider on the geolocation data it has collected on behalf of the publisher (knowledge of the audience and monetisation of spaces), the publisher is responsible for the processing and the provider of SDK its subcontractor;
- in the case of processing carried out by the SDK provider on its own account, the SDK provider is responsible for processing; once this processing uses data collected through the application, the publisher must be informed of the purpose of this collection and have given its consent to it before the SDK provider uses the data its own account. Any collection of consent must be carried out on the application before the data is collected;
- the provider of the operating system is responsible for the processing that it carries out in order to offer the precise geolocation calculation service to third parties, including in particular the publisher of the application.

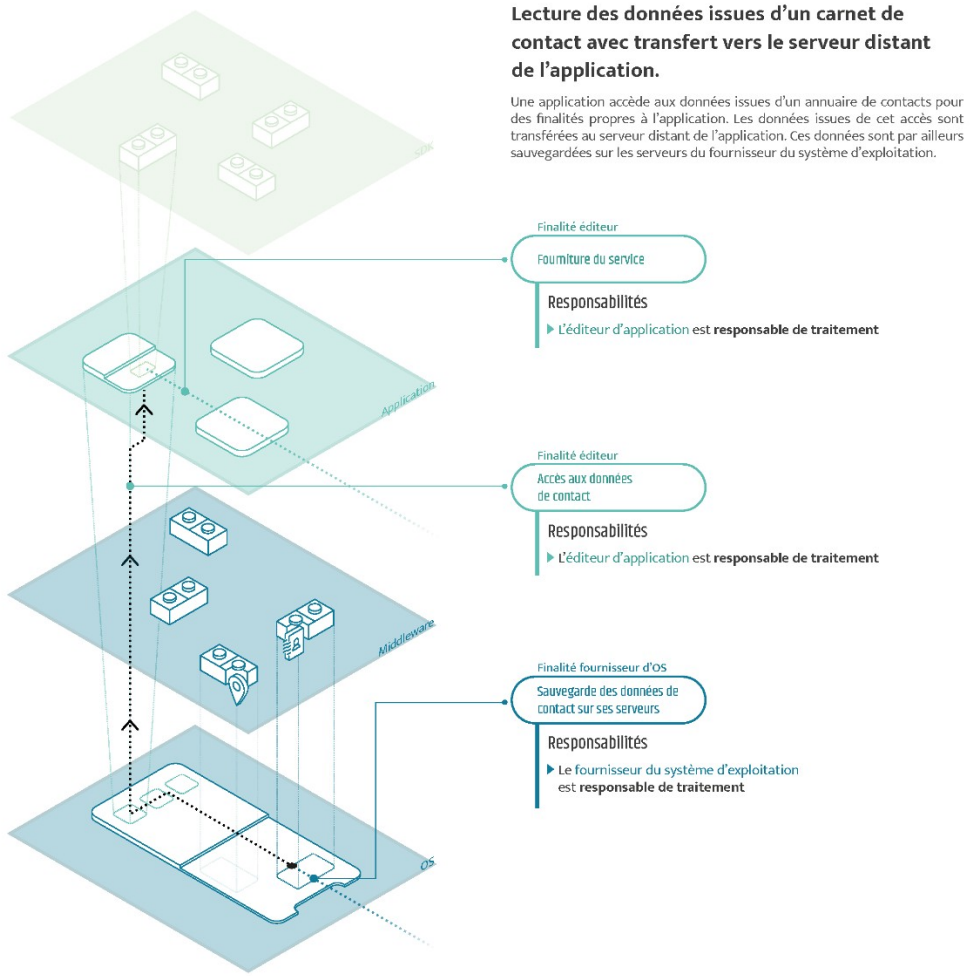


Read data from a contact book with transfer to the application's remote server

An application accesses data from a contact book for application-specific purposes. This data is stored on the servers of the operating system provider. This data is also transferred to the remote server of the application editor.

In that case:

- the publisher of the application must be regarded as responsible for the processing of such data (which constitutes a reading and/or writing operation within the meaning ofArticle 82 of the Data Protection Act) and the processing of data resulting from such access because it determines its purposes and means;
- for its part, the operating system provider is responsible for the processing of the user's data stored on its servers.



References

- Article 4 GDPR
- Article 82 of the Data Protection Act

5. Publisher-specific recommendations

Package leaflet

Who are these recommendations addressed to?

- These recommendations are addressed to **app publishers**.
- In the context of these recommendations, the publisher of the application is defined as the **legal entity (or the sole company of a natural person) that makes the application available to users** (most often through an application store) to offer its products or services.
- In practice, these recommendations are specifically addressed within the publisher:
  - the *Data Protection Officer (DPO)*;

- members of the team responsible for editing applications, in particular those responsible for their specifications (such as the product manager or *product owner*).

- If the publisher itself can proceed with the development of the application, it is common for it to rely on an external developer for this purpose. In this case, it is necessary to consider the role of the publisher as a client, the recommendations relating to the development activity itself are provided for in the specific recommendations to the developer. **In the event that the developer and publisher are the same entity, they are invited to consult simultaneously the recommendations applicable to the publisher and the developer**.
- These recommendations can also be usefully consulted by any partner of publishers or members of the public to assess the compliance of their approaches.

What is the purpose of these recommendations?

- These recommendations are intended to help publishers to ensure compliance with their various obligations under data protection regulations and thus the compliance of the processing of personal data they implement, throughout the life of the application.

How to use these recommendations?

- These recommendations are organised into several sections, each corresponding to a step in the provision of an application. Each thematic recommendation outlines the challenges of the design and operation of an application in terms of the protection of personal data, recalls the main obligations arising from the GDPR and the Data Protection Act, and brings together a series of tips and best practices to implement.
- A **consolidated checklist of key recommendations** for publishers is proposed at the end of this section. Publishers are invited to study this list and use it, in particular when drafting the contractual documentation, to ensure, where appropriate, that these recommendations are taken into account by their partners.

See also

Publishers are also invited to consult in this document the recommendations applicable to other actors, which may affect them incidentally, and in particular the following:

- Developer-specific recommendations
- Specific recommendations to SDK providers

5.1. Design its application

The consideration of the protection of personal data must start from the design phase of the applications. It is therefore the responsibility of the publisher, if necessary with the help of its partners, to clearly define the processing of personal data implemented.

1. Identify the existence of personal data processing

The first step of the publisher must be to identify whether personal data processing will be carried out through its application.

- **Is this indeed a processing of personal data**?
  - As a reminder, personal data (or, more succinctly, "personal data") is any information relating to an identified or identifiable natural person. For example, in the case of a mobile application, this can be the user's name and first name, but also his alias, geographical position, activity data in the application or even the technical identifiers of the device he uses.
  - In many cases, applications may offer the service sought without processing personal data (e.g.: applications flashlight, virtual bubble level, compass, calculator, chronometer or timer, metronome, tuner, certain games, etc.)
  - An application that does not process personal data does not fall within the scope of the GDPR.
  - The publisher should analyse the need to collect data for each processing and consider whether alternatives that do not process personal data are possible.

- **Can the processing be exempted from the application of the GDPR?**
  - Subject to certain conditions (referred to in part 4 of these recommendations: 'What are the roles of each actor in the use of the application?'), the processing may fall withinthe scope of the domestic exemption, without entailing liability of the application publisher within the meaning of the GDPR.
  - As a reminder, these conditions are cumulative compliance with the following two criteria:
    - the processing is carried out at the initiative, at the discretion and solely on behalf of the person (here the user of the application), i.e. decided and implemented by the latter;
    - the processing is carried out under the control of the person, that is to say in complete autonomy, in a compartmentalised environment, namely without possible intervention of third parties on these data: the publisher only provides the software to the user.
  - For each treatment, the publisher should prefer a configuration that meets the criteria of the domestic exemption, for example:
    - using local calculations instead of APIs querying remote servers,
    - by embedding resource bases within the application to avoid network queries,
    - using local data sharing tools between multiple user-controlled applications,
    - by enabling peer-to *-peer* communications between users without any storage or transit of personal data through a centralised server.

Point of attention

It should not be forgotten to include in the analysis treatments potentially carried out by third parties.

- **See part 5.2 of these recommendations: Mapping its partners**

2. Ensure legal compliance of processing

If, at the time of the design of the application, the publisher identifies that personal data processing will be carried out, each of these processing operations must comply with all the principles laid down by the GDPR and the Data Protection Act.

- **Is a purpose correctly defined for each processing operation?**
- **Is a legal basis identified for each treatment?** The publisher must identify a valid legal basis within the meaning ofArticle 6.1 of the GDPR. Processing carried out in the context of mobile applications may be based, inter alia, on consent, contract or legitimate interest:
  - Where the processing is based on consentc, the publisher must ensure that it is properly collected (see section 5.3 of these recommendations: "Manage consent and rights of persons".
  - The processing may be based on the legal basis of the contract only if it is objectively necessary for the contract entered into by the data subject.
  - The legal basis of the legitimate interest requires an analysis of the balance of interests between the user whose data is processed and the controller. In principle, profiling and personalised advertising cannot be justified by the legitimate interest of the publisher and requires consent[12].
- **Are accesses to the user's terminal implemented?**
  - The publisher must identify the reading and/or writing operations on persons' terminals within the meaningof Article 82 of the Data Protection Act implemented within its applications. These operations can correspond to a wide range of techniques.
  - In particular, in the context of mobile applications, mobile identifiers (whether advertising or non-advertising), results of operations to identify characteristics ('fingering'), unique identifiers, but also *hardware* identifiers, access to telephone sensors or data stored in the terminal (contact card, photographic gallery, etc.) are included.
  - Consent is not necessarily necessary for all readings or writings, since the texts provide for exemptions that depend on the purposes pursued. The operations necessary for the implementation of functionalities expressly requested by the user are thus not covered by this consent requirement. The publisher should provide precise instructions to the developer to identify which tracers and terminal accesses must be subject to consent.
  - To carry out the technical analysis of the operations implemented, and for which the publisher is responsible, the assistance of the developer is necessary.

[12] Opinion of the Article 29 Working Party on profiling and automated decision-making, WP 251, rev. 01 ' *[it] would be difficult for data controllers to justify the use of legitimate interests as a legal basis for intrusive profiling and tracking practices for marketing or advertising purposes, e.g. those involving the tracking of individuals on multiple websites, locations, devices, services or data brokering*'. Paragraph 56 of Decision No SAN-2023-006 of 11 May 2023: ' *Where the service requested by the user necessarily involves the processing of health data, it is however necessary that the user be fully aware that his or her health data will be processed and sometimes kept by the controller, which in principle implies explicit information on this point when obtaining consent.*'

<table>
<tr><th colspan="4">Read and/or write operations on the user's terminal are implemented</th></tr>
<tr><td>By default: The consent of the person is necessary

Examples:
• collection of the advertising identifier for advertising purposes
• collection of contact data for user discovery purposes
• collection of location for the purpose of recommending content</td><td colspan="3">By exemption: the consent of the person is not necessary</td></tr>
<tr><td></td><td>The sole purpose of the reading and/or writing operation is to enable or facilitate communication by electronic means

Example:
• use of identifiers for load balancing or routing purposes</td><td colspan="2">The operation is strictly necessary for the provision of an online communication service at the express request of the user</td></tr>
<tr><td></td><td></td><td>Functionality expressly requested by the user

Examples:
• GPS access to provide requested location functionality
• use of authentication identifiers</td><td>Use of security of the service, centered on the protection of the user

Examples:
• using tracers to prevent denial-of-service attacks
• using tracers to prevent credential stuffing</td></tr>
<tr><td></td><td></td><td></td><td>Limited audience measure

Example: simple counting of the number of daily users for the purpose of sizing the service</td></tr>
</table>

- **Is a data retention period associated with each processing?**
  - The data processed within the application must be kept for a period strictly necessary for the purpose pursued by the processing.
- **Is the collection of the personal data concerned necessary and minimised**
  - The publisher should identify the data to be collected for each processing, as well as the level of precision with which the application should process it in order to minimise the data processed (e.g.: it is best to store only the year of birth instead of the full date of birth if the application only needs the year).
- **Processing of sensitive data (within the meaning of Article 9 GDPR: are political, religious, health data, etc.) implemented?**
  - Such processing of sensitive data is prohibited in principle unless it is based on one of the exceptions provided for in Article 9.2 of the GDPR, such as the consent of the data subject.
  - In particular, any categorisation or creation of segments on the basis of such data, for the purpose of making such a profile and/or sending personalised advertising, must serve a legitimate purpose (Article 5 GDPR) and is in principle

not allowed. If considered and lawful in a certain context, the categorisation is subject to the prior consent of the customer concerned.
- If such processing is based on consent, this must be given prior to the processing of data in a free, specific and informed manner. Thus, the user must be able to decide freely and without constraint on the implementation of the processing. This choice must in principle be expressed in a specific way, for example by displaying a specific warning or information prior to the collection of consent or by adding a box to obtain separate consent[13].

- **How to protect the data of minors?**
  - It is common for publishers to publish applications that are aimed at minors. As they benefit from special protections under the regulations, it is important to implement additional measures to protect their personal data and respect their privacy.
  - Those recommendations do not deal specifically with the measures to be implemented as such; refer to the work published by the CNIL on the subject[14].

Point of attention

Potentially third-party treatments should be included in the analysis.

⇨ **See part 5.2 of these recommendations: Mapping its partners**

3. Apply data protection principles by design and by default

It is recommended that, for each of the processing operations envisaged, it is possible to implement technical and organisational measures to protect personal data by design and by default (so-called *"data protection by design and by default"* principles)[15]:

- **Is the envisaged processing of personal data essential for the provision of the service?**
  - Some of the planned treatments may not be essential to the provision of the expected service (e.g. geolocation can simplify a geographic search, but can be replaced by manual address entry).
  - The publisher should leave the choice to the end user to choose whether or not to use the features not strictly necessary for the proper functioning of the application.
  - The publisher should only impose the creation of an account if necessary, and consider alternatives to avoid collecting email addresses and passwords.

- **Are the application's default settings the least intrusive possible?**
  - The publisher should determine, for each treatment, the minimum parameters for providing the requested service (e.g.: it should not by default collect the person's location data if it only serves to facilitate the use of a search tool that can be functional without it).
  - If it identifies different categories of users, the publisher should analyse these parameters for each of these categories (e.g.: the e-mail address of individuals should not be systematically collected if it is useful only for paying users in connection with invoicing).

- **Does the design of the system make it possible by nature to protect the privacy of users?**

[13] "Digital rights of minors", cnil.fr
[14] Article 25 GDPR, cnil.fr
[15] " *Emerging privacy-enhancing technologies*", oecd-library.org

- The publisher should analyse whether privacy techniques can be applied to the treatments implemented.
- For a review of some of these techniques and examples of use, the publisher can refer to the related guides produced by the OECD[16] and the*Information Commissioner's Office* (ICO)[17], the UK data protection authority.

- **Does this design minimise risks to users?**

  - The publisher should, where possible, use end-to-end encryption mechanisms, which may reduce the scope of its responsibilities and limit the consequences in the event of data leaks.
  - The publisher should minimise the data transmitted to its partners and, if possible, do not transmit identifying data (name, alias, unique identifier number, etc.).

4. Document his analysis

Since the entry into force of the GDPR, controllers must take a continuous approach to the compliance of their IT systems through the implementation of internal mechanisms and procedures to demonstrate compliance with data protection rules.

Therefore, the principle of accountability of actors requires publishers to adopt certain tools and procedures prescribed by the GDPR to ensure compliance of their processing, in particular:

- **Maintain and keep up-to-date a record of treatments**. It is a steering tool that participates in the documentation of compliance, allowing to identify and analyse all the processing of personal data implemented and to identify and prioritise the associated risks. This should provide a global view of the data processed, what they are used for, who can access it, how long they are kept, if data transfers to third countries are planned, how this information is secured.
- **Justify and document the defined retention periods.** A retention period must be determined by the controller according to the purpose which led to the collection of such data.
- **A Data Protection Impact Assessment (DPIA) may be required where processing is likely to result in significant risks to individuals.**
- **The appointment of a data protection officer may be mandatory in certain cases**. In other cases, it is encouraged by the CNIL.

5.2. Mapping partners

It is common for all or part of the data processing carried out as a result of the installation of an application to be carried out not technically by the publisher but by third parties. It is therefore essential for the publisher, as controller, to have a complete vision and control of the roles and compliance of the measures implemented by its partners.

1. Mentoring relationships with developers

In the vast majority of cases, the publisher will call on a technical partner for the development of the application. It is essential to make an accurate analysis of this relationship.

- **Is the developer's qualification clear to both parties?**

  - The publisher should identify precisely and in advance the processing of personal data that will be implemented by the developer on behalf of the publisher in the context of the development and operation of the application. The developer will

[16] Chapter 5: Privacy-enhancing technologies (PETs) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance (PDF, 722 KB), Sept. 2022, ico.org.uk
[17] These obligations are developed in the Subcontractor's Guide published by the CNIL (PDF, 583 KB)

then act as the processor of the responsible publisher (see part 4 of these recommendations).
- UnderArticle 28 of the GDPR, the publisher must formalise this qualification and the obligations associated with it (*e.g. through a data processing agreement (DPA)*).
- Attention: if the developer implements processing on his own behalf, he or she may be qualified as controller for them (see part 4 of these recommendations, in particular: 'Developer qualification'). However, in its capacity as sponsor of the application, the publisher must be informed of these treatments and have accepted them, for example via the contractual elements.

- **Is the developer aware of his obligations as a subcontractor?**
  - The publisher must include, in the contract between him and the developer, all the particulars set out inArticle 28. It is recommended that the developer be made aware of[18]his obligations, and in particular that he must act only on instructions from the publisher.

- **Does the developer have the necessary elements to comply with his obligations?**
  - The publisher must provide clear instructions on the treatments to be implemented, for example via the processing register.
  - The publisher should set up a clear point of contact on privacy issues (e.g. DPO/DPO).
  - The publisher should give clear and documented instructions in terms of safety measurement and compliance processes (see section 6.4 of these recommendations, in particular: 'Ensure the security of the application').
  - The publisher should provide in the contractualisation a test of acceptance ('recipe') concerning compliance with these points.

2. Identify possible relationships with other third parties

If the developer is the publisher's main interlocutor in the realisation of an application, it is common for it to involve other third parties inthe processes implemented.

- **The publisher may refer to part 4 of these recommendations to identify all the treatments implemented by third parties in the context of the design and operation of the application.** This can be complex in the context of mobile applications, including processing related to third-party SDKs, calls to OS APIs, performance analysis, battery use or OS telemetry. The developer must be able to indicate to the publisher all the treatments implemented by third parties that he has included.
- **In particular, the publisher should ask its developer to implement the SDK selection mechanisms described in Part 7 of these recommendations ('SDK provider-specific recommendations')** since, as controller, the publisher will assume final responsibility for including an SDK in an application.

5.3. Managing people's consent and rights

For the processing that falls under its responsibility, the publisher must ensure that, in its interactions with individuals, the rights of individuals are respected, whether in terms of information, consent or the exercise of rights, even when the practical implementation of these rights is done by a third party.

[18] Articles 13 and 14 GDPR, cnil.fr

1. Properly inform its users

The first of these obligations is to properly inform the users of the application, an essential step to ensure transparency for any direct or indirect data collection[19].

- **What information is provided to users of the application whose data is being processed?** This information, usually grouped together in a document entitled 'Privacy Policy' should include:
  - mandatory elements underArticle 13 of the GDPR[20];
  - the mandatory or optional nature of each treatment (and how the refusal affects the use of the application);
  - the list of permissions to access the requested data, their mandatory or optional nature and the purposes pursued through these permissions.

- **How can information be made available to users?**

  - The publisher can use the page dedicated to the application in the app store to:
    - provide the privacy policy of the application,
    - indicate the main elements, in particular the identity of the publisher, the purposes of the processing and the manner in which the rights are exercised,
    - list the permissions required by the application and the purposes justifying access to the associated data. These permissions may be divided into two categories, depending on whether they serve only the service rendered by the application to the user or also pursue other purposes.
  - The publisher should ensure that the privacy policy is easily accessible:
    - before launching or downloading the application, for example on its website or on its download page. If possible, it should also be made available on the application page in the app store;
    - within the app, for example directly from its menu
  - The publisher should ensure that the privacy policy is concise, understandable by its audience using simple language and illustrated using visual elements. To adapt to the medium, a presentation of this information can be envisaged in two levels, with a first using icons and tables to make it understandable.
  - The use of a single privacy policy is not the only way to meet this obligation of information, and may often, in the context of mobile applications, fail to achieve the objectives in terms of simplicity and conciseness: it may be necessary to contextualise this provision of information during each specific collection and to use simplified presentation methodologies in this case[21].
  - While it is common for the OS to provide users with tools to inform them of the most intrusive collections (camera activity marker or geolocation), the publisher should consider in the application interfaces the reinformation of people about the access or sharing of certain particularly intrusive data (geolocation, contact book, microphone, etc.), for example through the use of persistent indicators when these features are enabled.

2. Obtain valid consent from users

If the legal basis chosen for a processing is that of consent, or if a reading and/or writing operation not subject to exemption is implemented underArticle 82 of the Data Protection Act, consent must be obtained.

- **How to obtain consent in the context of mobile applications?**

[19] 'Sheet No 12: Informing people', development team guide, lincnil.github.io
[20] '[Synthesise] Summary', design.cnil.fr
[21] "Websites, *cookies* and other tracers", cnil.fr

- The publisher must comply with the obligations in terms of the collection of consent specified by the CNIL in its guidelines and recommendations on *cookies* and other tracers when[22] a reading and/or writing operation is implemented.
- The publisher should take into account the specificities of the mobile interface, including the existence of permission windows and the limitations in terms of space available during this collection.
- The publisher should clearly explain his expectations to its developer.
- Since the publisher is responsible in the event of a breach of the obligation to obtain consent, it is essential that he implements measures to ensure proper compliance with his instructions. It may therefore consult Part 5.4 of these recommendations ('Maintain compliance during the life cycle of the application').

3. Enabling the exercise of rights

It is up to the publishers, controllers, to guarantee and respect the exercise of people's rights, taking particular account of the specific context of mobile applications

- **What rights should the publisher act upon?**
  - In the general case, the rights of persons are the right of access, the right to erasure, the right of opposition, the right to portability, the right to rectification and the right to restriction of processing[23].
  - Depending on the legal basis, some of those rights are not applicable[24].
- **By what means can it be followed up?**
  - If the texts do not provide a privileged means of responding to the exercise of rights, the publisher must analyse the most suitable methods for doing so. It is therefore recommended that persons be provided with a rights management centre within the application where all rights can be exercised. The publisher must ask his developer to advise him in this process.
  - It is essential, when contracting with the subcontractor(s), to ensure that the technical and organisational systems make it possible to respond to these rights, and in particular whether an automatic response is provided to them (e.g. via APIs to respond to requests for expression of rights).

[22] "File No 13: Preparing the exercise of people's rights', development team guide, lincnil.fr.github.io

[23] "Sheet No 15: Take into account the legal bases in the technical implementation. The exercise of rights and the information arrangements to be provided in accordance with the legal basis', guide of the development team, lincnil.fr.github.io

[24] "OWASP MASTG", mas.owasp.org

5.4. Maintain compliance during the life cycle of the application

Compliance measures are not limited to the design and publication of the application. The publisher, as the controller, must put in place a set of processes to control and ensure this compliance throughout the life cycle of the application.

1. Ensure the maintenance of security over time

If the publisher is not the actor directly implementing the security measures, it has, because of its role as controller, the responsibility to give precise instructions to its processors to ensure the security of the data.

- **How to express safety requirements?**
  - The publisher should formalise the expected technical measures in terms of security (Article 32 GDPR) of the data with the developer, specifying that these requirements are applicable to subsequent subcontractors. It may, for example, request compliance with the requirements formalised by the CNIL in Part 6 of these recommendations ('Developer Specific Recommendations').
  - The publisher should ensure that the contract with the developer provides for the update of the application in the event of a third party vulnerability or in the code.
  - The publisher must provide that the processors carry out the transmission of security alerts that may lead them to formalise a notification of a data breach (Article 33 GDPR) within a period consistent with the legal deadline for first notification of 72h to the data protection authority (in France, the CNIL).

2. Auditing compliance with partners' commitments

The publisher must use sufficient and appropriate means to monitor compliance with its instructions in terms of privacy.

- **How to implement audits?**
  - The publisher should remind in the contractual documentation that the developer is required to assist him in conducting audits (Article 28 GDPR).
  - For example, the publisher can use the *OWASP Mobile Application Security Testing Guide* (MASTG)[25] proposed by the NGO Open Web Application Security Project as a basis for analysing the security of its application.
  - The editor can use a static analysis tool. These tools make it possible to verify that the included SDKs and the requested permissions correspond to their instructions. In case of doubt, the publisher should ask its developer to justify the observed elements (SDK included, permissions requested, etc.). Some tools offer further analysis, including security issues.
  - The publisher may set up (or hire a third party provider for this purpose) a test bed to verify the proper functioning of the consent collection tools implemented. To that end, he may:
    - Equip a test phone or emulator for interception of network communications.
    - Test its application, and ensure that no symptomatic requests for tracer use are issued until consent is actually obtained.
  - Due to the great complexity of certain application bricks, these arrangements cannot allow them to ensure compliance with the obligations and are only a complement to organisational measures (see section 5.2 of these recommendations: 'Mapping partners').

[25] Deliberation No 2021-122 of 14 October 2021 adopting a recommendation on journaling and 'The CNIL publishes a recommendation on logging measures', cnil.fr.

3. Implement robust processes in terms of compliance

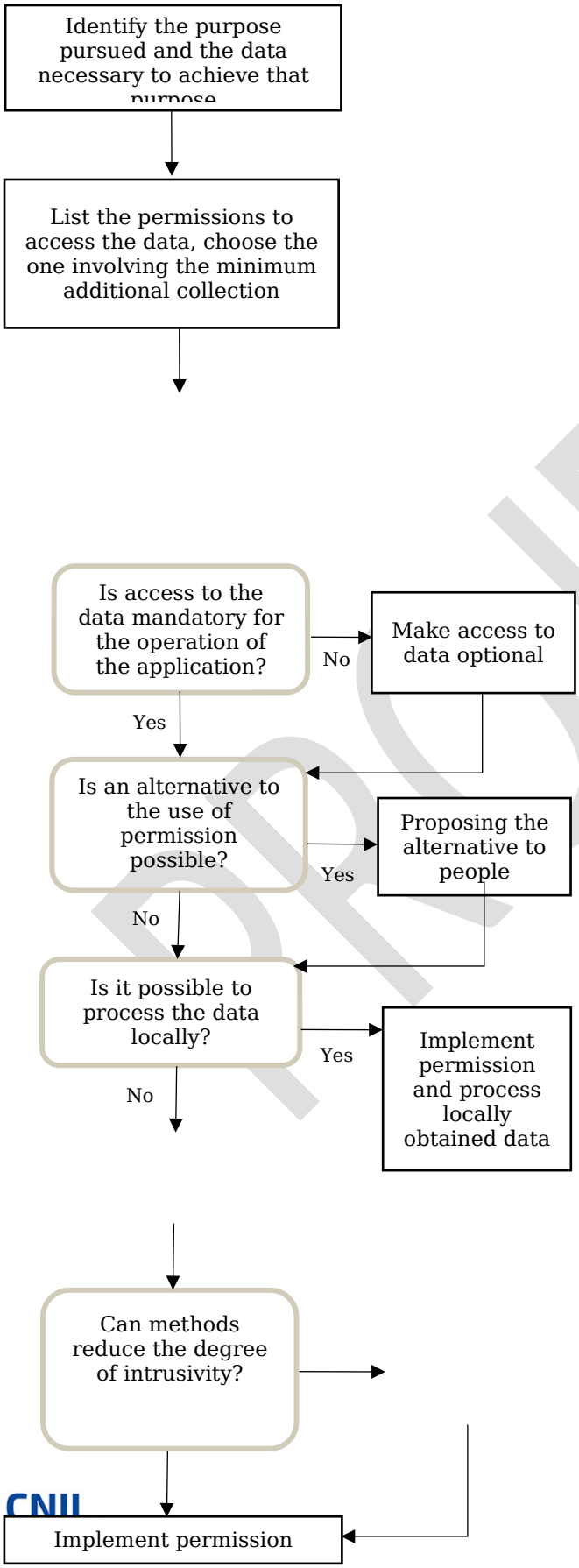
Decisions that may impact the compliance of an application can be made after the initial development of the application. In order to ensure that the necessary level of compliance is maintained, processes must be designed upstream and then implemented appropriately (on a regular basis or when significant development is undertaken).

- **Is the monitoring of possible changes in data processing carried out?**
  - It is desirable for the publisher to put in place a validation process so that any evolution affecting the conditions of implementation of the processing (sub-processor choice, SDK, functionalities, collection of consent) is approved by the latter. These choices can frequently be confirmed during maintenance operations: the publisher should ensure that their process takes this into account.
  - The publisher must update the register of processing operations in order to take into account developments in the data processing implemented, as well as the data privacy policy.
- **Are processes in place to ensure the confidentiality of data?**
  - The publisher must supervise access to personal data by subcontractors. A good practice is to implement logised access controls to avoid internal diversions (personal or structural), as mentioned by the CNIL in its recommendation on logging[26]. The use of fictitious or synthetic data by subcontractors is an alternative solution.
  - The publisher should supervise and verify the deletion of data whose retention period has expired.

[26] Thus, in its Decision 1/2021 adopted on 28 July 2021, concerning the dispute relating to the draft decision of the Irish Supervisory Authority concerning WhatsApp Ireland pursuant to Article 65(1)(a) GDPR, the EDPB found not only a breach of Article 14 concerning the collection of non-users' data, but also that due to the non-validity of the anonymisation process used, that violation persists for the processing of non-users' data in the form of lists of non-users after application of the loss hashing procedure.

5.5. Permissions and data protection by design

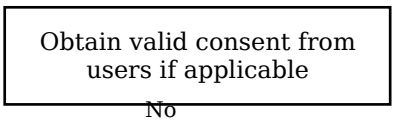
When developing an application, the choice of access permissions ('permissions') to use and the implementation of the associated data processing is a crucial step for the protection of individuals' privacy.



1. Use permissions

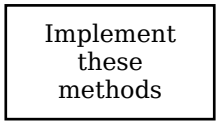
- **How to analyse permissions in view of the applicable texts?**
  - Permissions in itself do not necessarily entail an obligation within the meaning of the texts and constitute an independent technical measure. Thus access to a resource via a permission request, if that resource is then dealt with in a purely local way, may fall within the scope of the domestic exemption. Similarly, in this context, the conditions for the applicability of Article 82 of the Data Protection Act may not be met.
  - In addition, they do not require prior consent where access to information in the terminal is necessary either for the operation of the electronic communication protocol or for the provision of the service expressly requested by the user. However, in many cases (and as soon as the accessed resource is not processed locally), consent may be required as a result of Article 82. Part 5.3 of these recommendations "Managing consent and rights of individuals" explains these cases. The CNIL encourages the practice of providing that the application must systematically obtain the user's "permission" to access certain sensitive resources stored on the terminal (geolocation, contact book, cameras and photographs/films, etc.), regardless of the legal obligations resulting from Article 82 of the Data Protection Act.

- Similarly, remote access to a resource protected by permission may trigger a processing whose legal basis is consent.



- **What information should be given when collecting consent for permission?**

- In cases where consent is the rule, it is essential to obtain valid consent. Practical difficulties may arise in the articulation between consent and permission (see section 6.2.3 of these recommendations: 'Participate in compliance with the use of tracers and the collection of consent')



- It is also necessary to indicate in a clear and intelligible manner whether the functionality related to the requested permission is (i) necessary for the operation of the application, (ii) relating to the activation of an ancillary function for the benefit of the user (facilitating its navigation, allowing the scanning of a QR code, recording a voice memo) or (iii) relating to processing carried out for the benefit of the publisher or a third party distinct from the provision of the service rendered by the application (advertising value). If several purposes of different natures are pursued, it is important to respect the granularity of consent.

No

- **How to implement a permission selection process?**

- To ensure a data protection approach by design, a procedure for selecting permissions should be implemented following the steps described in the diagram opposite.

2. Practical Uses for Permission Selection

- **How to manage the use of geolocation?**

- The publisher should identify, among the permissions made available by the OS, the one that corresponds to the minimum level of granularity that is necessary for it:
  - approximate rather than precise location,
  - a one-time limited permission rather than a permanent permission,
  - only active permission when the app is in the foreground rather than permanently,
  - a permission that does not transmit information to third parties where possible (e.g. permission based on GPS alone and not analysis of the network environment).
- Where possible with regard to the service rendered, the publisher should propose an alternative to the use of this permission, for example the manual entry of a postal code or address instead of processing the person's geolocation data.
- If possible, the publisher should process the location data locally. For example, to find the place closest to its user among a list of places, the publisher should integrate the list in question into the content of the application and calculate locally the nearest location based on the person's location.
- Where applicable, the publisher should obtain valid consent for the remote collection of the person's location data. If consent is not obtained, it should consider the alternative methods identified above. Before sending location data to the servers of the application, the publisher should identify the minimum level of accuracy that is necessary to achieve its purposes and truncate the coordinates locally according to it.
- Generally speaking, the publisher should not keep the location data it used on a remote server but prefer its local storage in the application to repropos it to the user (via an item: "My last location").

- As a matter of principle, and except for applications whose operation depends on continuous localisation (navigation, some specific games in the public space), the publisher should not collect location when the application is not actively used by the user.
- In the event that the permission given by the user is permanent, the publisher should think of reminding him of the existence of the permission in a visible way in the interface of the application and asking him at regular intervals to confirm his consent to the location to be collected.

- **How to manage access to contact data stored within the user's terminal?**
  - The publisher should determine precisely the need and the reasons for accessing this contact data, and in particular whether it is mandatory for the operation of the application.
  - The publisher should identify the least intrusive associated permission. In particular, if he only wants to read the data, he should not ask for writing rights.
  - For any access permission involving the selection of a contact in a local way, it is excluded from making this selection other than directly on the user's terminal.
  - If certain access permissions require the pooling of contact data between several users of the application (for example, the discovery of contacts registered with an email), it is essential to collect consent for the reading of these contact data on the user's terminal and to ensure the information of all the persons likely to be affected by the processing[27]. The publisher should ensure that the user is properly informed about the nature of the collection and its intrusivity and, in the event of refusal, propose alternative methods (e.g.: manual number entry by the person for spot check of presence). If such alternatives are implemented, it should ensure that these tools cannot be misused, for example by capping the number or frequency of possible queries to avoid multiple automated queries for data suction purposes ("scattering").
  - In the previous case where the designer of the application wishes to show to the user which of his contacts already has the application in order to offer him to connect it, the following operations should be implemented:
    - Upon registration, each user of the application should consent to their own contact details being used in the future to be identified on third-party devices or to be found by third-party user accounts that have their contact details;
      - In that regard, it is not possible to consider that granting permission to access telephone 'contacts' is consent to the use of its own contact details by third parties;
      - If the user consents, the CNIL recommends that the parameter relating to the ability to be identified or searched be configured **by default** to the smallest possible level. The user should have the choice between several settings options ("Only me", "Friends", "Friends of friends", "All registrants", "Everyone, including non-registrants", etc.).
    - Access and analysis of the entire contact book should use the most suitable methods to limit the intrusivity of this processing (e.g. via *Private Set Intersection* techniques).
    - The contact data that would have been stored should be deleted at the end of the analysis and a new agreement for the use of this permission should be requested for any new access. Otherwise, it is recommended to set a limited period of consent to access terminal contacts for this purpose of comparison with the contact books of other users.

- **How to manage the use of the microphone?**

[27] 'Controller and processor: 6 best practices to respect personal data', cnil.fr

- The editor should determine precisely the need and the reasons for accessing the microphone, and in particular whether it is mandatory for the operation of the application.
- The publisher should identify the least intrusive associated permission (especially in terms of the possibility of competing audio stream capture, which may pose a significant risk to the person).
- If the need is punctual, the publisher should revoke the permission after recording the sound.
- If possible, the editor should offer alternatives to microphone access (for example, as part of a voice note-taking application, the editor should also offer a manual note-taking).
- Where possible, the publisher should process the audio content locally (e.g. if it offers a tuner, it should focus on using local phone computing capabilities over remote content processing).
- Otherwise, the publisher should obtain valid consent for the remote collection of data present in such audio content, ensuring that the person understands that the content will be sent to its servers. If consent is not obtained, it should consider the alternative methods identified above.
- If the use of the microphone is only useful for certain actions in the application (e.g. save a message), the editor should alert the user when the microphone is activated, for example through a clearly identified and dedicated icon.
- Before sending audio content to the application's servers, the publisher should offer its users to truncate or re-listen the shared content.
- Generally speaking, the publisher should not keep audio content collected on a remote server unless there is a specific and justified use. In particular, it should make the implementation of remote server backups optional, and to this end obtain the free, specific and informed consent of the users concerned.

- **How to manage the use of the camera?**
  - The editor should determine precisely the need and the reasons for accessing the camera, and in particular whether it is mandatory for the operation of the application. In particular, it should distinguish between access to the camera itself or access to photographs taken by the person and stored within his or her terminal.
  - On the basis of this need, the publisher should identify, among the permissions provided by the OS, the one that poses the least risk to the person, and in particular:
    - exclude the use of permissions requesting access to all of the user's multimedia content if the processing does not require such full access in relation to the purposes he pursues. On the contrary, it should rely on permissions that enable the user to select specifically the content he wishes to share with the application;
    - where a live photo or video is needed, give preference to solutions delegating such capture to system applications;
    - if this is not possible (e.g. for interactive uses of the video stream), make sure to require only the strict minimum in terms of hardware permissions (e.g. do not activate audio recording if this is not a necessity).
  - Where possible, the publisher should propose an alternative avoiding access to the user's camera.
  - If possible, the publisher should process the data locally (for example, if it offers editing tools, consider using the phone's local computing capabilities rather than remote image processing). Similarly, the editor should delete the metadata associated with the image (geolocation, timestamp, EXIF data) if they are not necessary.

- Otherwise, the publisher should obtain valid consent for remote collection of images. If consent is not obtained, the publisher should consider the alternative methods identified above.
- Before sending images to their servers, the editor should analyse the need to obtain the entire image. Otherwise, it should offer selection or blurring tools to the user.
- Generally speaking, the publisher should not keep the images collected on a remote server except in case of precise and justified use. In particular, it should make it optional to implement backups on a remote server, and obtain free, specific and informed consent from users for this purpose.

5.6. Checklist

Category	Sub-Category	Identifier	Description
Design its application	Identify the existence of personal data processing	1.1.1	Any operation that may be carried out shall be carried out without processing personal data.
		1.1.2	Any treatment that may be carried out is carried out locally.
	Ensure legal compliance of processing	1.2.1	Each processing operation has an identified legal basis.
		1.2.2	Read and/or write operations on people's terminals implemented within applications are identified.
		1.2.3	A data retention period is associated with each processing.
		1.2.4	No unnecessary data collection is carried out. The necessary ones are minimised.
		1.2.5	Sensitive data processed are identified.
		1.2.6	Additional measures are applied on the data of minors.
	Apply data protection principles by design and by default	1.3.1	The list of minimum treatments to provide the requested service is determined.
		1.3.2	The default settings only have the effect of implementing processing from this minimum list.
		1.3.3	The possibility of integrating privacy mechanisms is explored from the outset.
		1.3.4	The possibility of implementing privacy techniques, such as end-to-end encryption, has been explored.
	Document his analysis	1.4.1	A register of processing operations is carried out.
		1.4.2	Retention periods are justified and documented.
		1.4.3	A DPIA is performed if the treatment meets the criteria.
		1.4.4	A data protection officer is appointed within the publisher.
Mapping	Mentoring	2.1.1	The qualification of the developer is

partners	relationships with developers		agreed between the developer and the publisher.
		2.1.2	All references to Article 28 GDPR are included in the contract with the developer.
		2.1.3	The processing register is made available to the developer.
		2.1.4	The instructions given to the developer on the treatments to be implemented are clear and documented. An acceptance test (recipe) is included in the contract with the developer. A contact point dedicated to privacy issues is made available to the developer.
	Identify possible relationships with other third parties	2.2.1	All third parties involved in the application are analysed to identify whether they process personal data.
		2.2.2	Any SDK implemented is analysed to identify whether it processes personal data.
Managing people's consent and rights	Properly inform its users	3.1.1	A complete privacy policy is written.
		3.1.2	The privacy policy is accessible before downloading or installing the application. The privacy policy is also accessible within the app.
	Obtain valid consent from users	3.2.1	The obligations in terms of obtaining consent as explained by the CNIL in its guidelines and recommendations on *cookies* and other tracers are implemented.
	Enabling the exercise of rights	3.3.1	An analysis of the rights applicable to persons is carried out (right of access, right to portability, right to limitation, etc.).
		3.3.2	The provision of a rights management centre within the application is envisaged.
Maintain compliance during the life cycle of the application	Ensure the maintenance of security over time	4.1.1	The requirements in terms of expected technical measures are formalised with subcontractors.
		4.1.2	The vulnerability update process is contracted with third parties.
		4.1.3	The obligations in terms of security alerts to enable the notification of personal data breaches are reminded to the subcontractors.
	Auditing compliance with partners' commitments	4.2.1	Where the risks warrant, audits shall be carried out with subcontractors to monitor compliance with the instructions given. The audits to be carried out shall be explained in advance.

	Implement robust processes in terms of compliance	4.3.1	Instructions are given to subcontractors to ensure that any changes affecting privacy issues are approved before implementation.
		4.3.2	Updates are reflected in the Processing Register and Privacy Policy.
		4.3.3	Personal data are protected and their access is logged to avoid diversion.
		4.3.4	The deletion of data whose duration has expired is organised.
Permissions and data protection by design	Implement an approach for the selection of permissions	5.1.1	For each data whose collection is required, the permission involving the least additional data collection is chosen.
		5.1.2	The collection of non-mandatory data for the operation of the application is optional.
		5.1.3	Alternatives to the use of permissions are offered to individuals where possible.
		5.1.4	The collected data are processed locally where possible.
		5.1.5	Consent is validly collected when necessary (see 3.2.1).
		5.1.6	Before any remote collection, the accuracy of the data is reduced to the minimum necessary.

6. Developer-specific recommendations

Package leaflet

Who are these recommendations addressed to?

- These recommendations are addressed to **application developers**.
- The developer of the application is defined as **the legal entity or sole proprietorship that carries out the technical operations of developing the application, on behalf of and on the instructions of the publisher**.
- In practice, these recommendations are specifically addressed within the developer:
  - the *Data Protection Officer* (DPO) of an application development agency;
  - project managers responsible for the development of applications;
  - to the members of the team responsible for the development of applications.
- Although the developer acts in the majority of cases as executing publisher instructions, in practice, it supports a number of technical choices that have strong impacts on the characteristics of the treatments that will be implemented. **In the event that the developer and publisher are a single entity, they must simultaneously consult the recommendations applicable to the publisher and the developer**.
- These recommendations may also be consulted by any partner of the developer or interested third party to assess the compliance of the developer's steps.

What is the purpose of these recommendations?

- The developer makes a number of technical choices during the design and development of the application that could have a strong impact on the processing of personal data that will be implemented by the publisher.
- As such, it is essential that the developer implements an approach to ensure the publisher's information and approval regarding the technical choices made and their implications, and thus respects his duty of advice. **These recommendations are intended to help the developer in this process, throughout his activity of development and maintenance of the application.**

How to use these recommendations?

- These recommendations are organised into several sections, each corresponding to a stage in the development activity of an application. Each section outlines privacy issues and brings together a series of recommendations and best practices to be implemented by developers.
- A **consolidated checklist of key recommendations** for developers is proposed at the end of this section. Developers are invited to study this list and use it in particular when drafting their contractual documentation to ensure, where appropriate, that these recommendations are taken into account by their partners.

6.1. Formalise your relationship with the publisher

The central relationship in the design and development of an application is the one that binds the publisher and the developer. It is essential that aspects relating to the protection of users' personal data are at the heart of the construction of this contractual relationship. Note that if only direct relationships between publishers and developers are addressed here, the use of subsequent subcontractors (e.g. providers hired by developers) will require the cascading consideration of these recommendations.

1. Identify the responsibilities and obligations of each

The contractual relationship between the controller (publisher) and the processor[28] (developer) must be based on a clear understanding of the responsibilities of each.

- **Will processing be carried out on the basis of the subcontracting of personal data**?
  - The developer may refer to part 4 of these recommendations to determine his qualification under the GDPR. As a reminder, the fact that the developer makes certain technical choices does not necessarily make him the controller: a processor may determine the 'means' of processing as long as they are non-essential[29].

- **What requests do the publisher** make?
  - The developer should ask the publisher to provide, as an integral part of the specifications, the register of treatments concerning the application to be developed. In the event that this register of processing operations does not yet exist, the developer should request the provision of a comprehensive and clear specification, which allows to define which data will be used and thus subsequently implement a register of processing of the application.
  - When contracting with the publisher, the developer should ask the publisher for a clear qualification of his role for each of the treatments concerned. As a developer, it will act as a processor if it intervenes on data processing on behalf of and on instructions from the controller, but it is its responsibility and that of the publisher to determine the most appropriate qualification for each processing.
  - The contract of subcontracting between the publisher and the developer, in accordance withArticle 28 of the GDPR, must in particular stipulate the conditions for the implementation of each processing.
  - A contact point must be provided for by the contract to validate the choices having an impact on the processing of personal data: this is usually the publisher's DPO.

- **What obligations on the developer's side?**
  - As a subcontractor, the developer is responsible for a number of obligations underArticle 28 of the GDPR, detailed in this section, and in particular:
    - an obligation of transparency and traceability;
    - the obligation to take into account, as part of its duty of advice, the principles of data protection by design and by default;
    - the obligation to assist his client in complying with his obligations under the GDPR (see section 6.2 of these recommendations, 'Assume his role as an advisor to the publisher');
    - the obligation to guarantee the security of the data processed (see section 6.4 of these recommendations 'Ensure the security of the application').
  - In accordance withArticle 30.2 of the GDPR, the developer must keep a register of the processing activities carried out on behalf of the publisher, which must be made available to the publisher.

[28] EDPS Guidelines 07/2020 on the concepts of controller and processor (PDF, 1.6 MB), edpb.europa.eu

[29] "Transfer of data outside the EU", cnil.fr

- The developer must ensure that the personal data that he collects and processes according to the instructions of the publisher corresponds to those of the processing register or the complete specifications communicated by the publisher. Otherwise, it should alert the editor so that this document is updated.
- In any case, the developer is obliged to act strictly on documented instructions from the controller, by validating the possible use of further processors in accordance withArticle 28 GDPR.
- If the subsequent processors recruited by the developer carry out reading and/or writing operations, they may be jointly responsible or responsible for processing with the publisher in relation to these operations (see Part 4 of these recommendations: What are the roles of each actor in the use of the application?): the use of these providers and their qualification within the meaning of the GDPR and the ePrivacy Directive will have to be validated by the publisher.
- Finally, with regard to developer-specific environments (e.g.: technical environment for development shared between its clients):
  - The developer must determine his responsibility if any processing is carried out by him, and must then comply with all the obligations of the controller. This may be the case in particular if test data is used for the different applications developed by the developer.
  - The developer does not re-use the data which it holds as a processor, for its own purposes, only with the prior consent of the publisher (see Part 4 of these recommendations, 'What are the roles of each actor in the use of the application?').

2. Implement project management processes approved by both parties

- **What decision-making process?**
  - If a decision affecting users' privacy (technical choice, interface design, etc.) is identified by the developer, the developer cannot make this decision alone but should instead involve the publisher in the decision-making process.
    - In that regard, it is necessary to distinguish, on the one hand, the testing and development environment of the developer, in which the developer may be required to carry out data processing tests or SDK integration tests, at the request of the publisher or on his own initiative, and, on the other hand, the recipe environment in which the publisher is offered a version of the application in accordance with its instructions, including only the intended treatments.
    - The point of contact established within the publisher for this purpose should be used to facilitate communication.
  - The developer should present, as part of his duty of advice, the issues at stake in a clear manner and request that written instructions be sent to him, in order to be able to demonstrate that he is acting on instructions from the controller.
  - Particular attention should be paid to the following topics:
    - choice of partners and in particular the SDKs used (see section 6.3 of these recommendations: "Making good use of SDKs");
    - choice of permissions to be requested by the application and possible alternatives in case of refusal;
    - choice of how users may obtain their consent;
    - informing users and exercising their rights.
- **What processes to ensure compliance of personal data processing over time?**
  - The decision-making process described above should be maintained throughout the life of the application, in particular as a result of an external evolution or an alert (e.g. updating an SDK, detecting a security flaw). In these situations, the impact these developments may have on the data processing implemented

should not be overlooked. Some tools can help the developer analyse partners' terms of use updates.
- In the event of possible changes in the conditions for the implementation of the treatments, the publisher should be proactively informed. For example, if changes in the permissions proposed by the OS make it possible to better protect people, the CNIL recommends suggesting an update to the publisher, as part of its duty of advice.

- **What management for the publication of applications?**
  - If the responsibility for publishing an application or its updates in an application store rests with the publisher, it is common for this operation to be carried out in practice by the developer, in particular due to technical restrictions imposed by app store providers.
  - As such, the developer should ensure that he has all the necessary elements to ensure the correct information of the people in these stores and, if not, should ask the publisher to forward them to him.
  - The application's online account should be secure, excluding any password sharing.
  - If the developer is instructed to distribute the application without going through an app store, it should ensure that it has the ability to ensure the integrity of the distributed content.

3. Identify all processing of personal data

If the majority of the treatments will be listed in the register provided by the publisher or in a comprehensive specification, some development choices may involve the implementation of additional treatments. It is essential to identify and qualify the responsibilities of each with the publisher for all these treatments before their implementation.

- **Will personal data processing be involved in the use of functionalities made available by the AOS?**
  - The developer should analyse, when using tools provided by the OS, whether their use involves the processing of personal data.
  - For example, when using data backup features (sometimes enabled by default), it should inform and assist the publisher in the qualification of this processing and related issues (e.g. data transfers outside the European Union, as defined in Chapter V of the GDPR[30]).
  - The developer should analyse in this way all the APIs provided by the OS (notification, payment, *single sign-on authentication*, system health monitoring, security, fault management, etc.), to ensure that it does not implement processing without instructions from its controller.
  - It is recommended to monitor the evolution of OS and its functionalities, in particular in terms of minimising the processed data.
- **Are treatments implemented as a result of SDK integration?**
  - The developer should analyse, when using SDKs, whether their use involves the processing of personal data (e.g. the collection of a hardware-specific unique identifier, the collection of IP addresses, surrounding Wi-Fi identifiers, etc.).
  - If this is the case, it should inquire about their characteristics to allow the qualification of these third parties within the meaning of the GDPR. It may refer to Part 4 of these recommendations ("What are the roles of each actor in the use of the application?").

[30] The contract between the publisher of the application and its developer may, in particular, be invalid if the non-compliance with the obligations of the other party under the GDPR constitutes an error as to the essential qualities of the subject-matter of the contract (see, to that effect, CA Grenoble, 12 Jan. 2023, No 21/03701, in the case of website design).

- The information that should be collected in this regard concerns in particular the list of personal data collected and the purpose, nature and purpose of the processing carried out on such data according to the configuration of the chosen tool. In case of absence of these elements, if doubts remain as to the treatments actually involved in the use of the SDK, the developer should inform the publisher, and consider waiving the use of the SDK. **In any case, these additional treatments cannot be implemented without the information and prior consent of the publisher.**
- This analysis should be applied to all SDKs used, including those provided by the OS provider.

6.2. Assume its role of advising the publisher

The developer, as a processor within the meaning of the GDPR, is obliged to assist and advise the publisher in its compliance with certain obligations imposed by the GDPR, particularly with regard to the implementation choices that fall within its expertise. It must ensure that the controller is informed of the technical choices made and their implications, for which the developer is contractually liable. To this end, he may propose ways of processing personal data in order to ensure that the rights of individuals are respected. . To this end, he may propose ways of processing personal data in order to ensure that the rights of individuals are respected.

1. Propose developments respecting the principles of protection of personal data

The developer must propose implementation modalities and provide advice taking into account the principles of minimisation and data protection by design and by default.

- **Is the principle of data minimisation taken into account?**
  - Whether subcontractor or simply providing the code to the publisher, the developer should ensure that the processing he proposes to implement on behalf of the publisher respects the principle of minimising the collected data. It can also technically advise the publisher to choose and implement more protective solutions. The CNIL recommends:
    - the use of privacy protection techniques (e.g. as described in a guide on the subject produced by the ICO[31]);
    - the use of methods to perform data operations and calculations locally within the terminal, instead of using remote APIs.
  - The developer should analyse the publisher's instructions to identify whether the data he is asked to process is indeed necessary, and, if not, propose to exclude certain data from the processing.
  - If the developer identifies that certain data is accessible by third parties (e.g. the OS or SDK), solutions should be proposed to limit the risks of such access. In a non-exhaustive manner, the CNIL makes the following three recommendations in particular:
    - the data displayed in the notifications issued by the application may be limited, simply indicating that these are available within the application. As soon as possible, the content of the notifications should be encrypted, so that the OS provider is not able to access them;
    - the contents of the backups can be encrypted, allowing the user of the application and himself to retain control over the cryptographic keys used for this encryption;
    - the transmission of interapplication identifiers to SDK providers should be avoided. If this transmission is necessary, a hash of the identifiers should be carried out beforehand.
    - the developer should ensure that any permissions requested are strictly necessary for the operation of the application and the purposes of the processing, in order to be able to advise the publisher on ways to minimise the collection allowed according to permission levels. Where possible, alternative and voluntary data collection methods should be provided for by the user if they are refused (see section 5.5 of these recommendations: 'Authorisations and data protection by design').

. To this end, he may propose ways of processing personal data in order to ensure that the rights of individuals are respected. Chapter 5: Privacy-enhancing technologies (PETs) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance (PDF, 722 KB), Sept. 2022, ico.org.uk

[31] ' *Cookies* and other tracers: the CNIL publishes amending guidelines and its recommendation', cnil.fr

- For the most intrusive permissions, it is recommended that the developer plan to report to the user when they are active, via OS features or within the app.
- If the developer chooses to activate certain permissions as soon as the application is installed, he should ensure that this choice is compatible with the need to obtain valid consent before any reading and/or writing operation, in connection with the publisher (see section 6.2.3 of these recommendations: 'Participate in compliance with the use of tracers and the collection of consent').

- **Are sensitive data within the meaning of Article 9 GDPR processed?**

What is sensitive data within the meaning of Article 9 GDPR?

- **See Part 5.1 of these recommendations:** " Ensure the legal conformity of processing operations"

- If the instructions provided by the publisher involve the processing of sensitive data, a clear distinction should be made between these types of data and the others, in particular at the level of the architecture of the service.
- If the developer identifies that sensitive data processing is being carried out without having been instructed to do so, the publisher should be informed so that the latter can analyse the compliance of the processing. Otherwise, it is prohibited as a matter of principle.
- Particular attention should be paid to the processing of these data, since their processing is subject to a specific procedure, in particular in terms of the transmission of such data to third parties. For example, when integrating SDK, the developer should ensure that they have no access to this data in principle.
- The publisher should be alerted in case of irrelevant or even unlawful use of sensitive data, either by design or by mistake (e.g.: use of sensitive data to target advertisements).

2. Help to ensure that users' rights are respected

The developer has an important role to play in respecting people's rights. As such, when designing the application, it must ensure that the rights can be effectively exercised within the application. If it has the quality of subcontractor, it must assist the publisher in the management of user requests.

- **Are users well informed?**
  - The developer should remind the publisher of the need to make available the privacy policy provided by the publisher within the application. It must be readable on a mobile medium (see recommendations made under this heading) and easily accessible (e.g.: displayed on the main app menu, or at the person's account page for an authenticated application). When there are general terms and conditions of use of the application, a specific document or link to access the privacy policy is in principle necessary.
  - In addition, a simplified GDPR information screen can be made available at the first launch of the application, in order to guarantee complete information to people before using the application.
- **Is the exercise of rights possible within the application?**
  - The developer should think about the exercise of rights by design, especially in terms of structuring databases. In particular, the right of deletion if expressed must be respected, regardless of technical constraints.
  - To the extent that the collection takes place in the context of mobile applications, it is recommended that the developer propose to the publisher to offer users to exercise their rights directly within the application, through a dedicated page. In particular, this would allow the publisher to avoid collecting additional data to

respond to the exercise of rights (by simply using the identifiers used for the collection in order to implement it).

- The developer must ensure that, when these rights are exercised, all the data concerned is transmitted to the person. This requires, if processing is carried out by third parties such as SDKs and if the publisher wishes to provide an automatic response to requests, these third parties provide rights management APIs to make it possible to automate the process.

3. Participate in compliance with the use of tracers and the collection of consent

In the event of the use of tracers, it is essential that the publisher can study the possible need for consent[32]. It is therefore recommended to the developer, as part of his duty of advice, to alert the publisher if elements of the specifications involve the implementation of reading and/or writing operations, and to the extent possible, to participate in the proper implementation of the collections of consent. For more details on the contexts in which consent may be required, see section 5.1.2 of the recommendations addressed to publishers, in particular 'Is access to the user's terminal implemented?'.

- **How do I collect consent in the context of mobile applications?**
  - Consent, in the context of mobile applications, must meet the level of requirement described in the recommendation " *Cookies* and other tracers" published by the CNIL, from which the diagrams below are extracted.
  - However, it is necessary to adapt the interfaces to allow the readability of windows in a mobile environment.

Figure 1- The details of the purposes are available under a scroll button that the user can activate on the first level of information

[32] "Safety recommendations relating to TLS", ssi.gouv.fr

Figure 2 – The details of the purposes are available by clicking on a hyperlink present on the first level of information

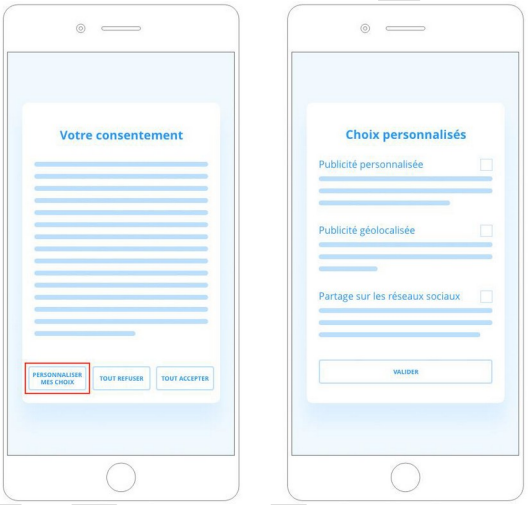


Figure 3 – The possibility of granular consent may be offered on a second level of information via a "personalise my choices" button inserted on the same level of information (first level) as the buttons to "accept everything" and "deny everything".

- To avoid the fatigue of consent and make the collection of consent more understandable for ut2ilisers, it is recommended to collect consents in a contextual way based on the actions taken instead of a single initial screen.
- The arrangements for obtaining consent must be agreed with the publisher and put in place within the application on the basis of its instructions. The developer should document this approach.

- **How to articulate consent and permissions?**

  - As part of mobile applications, developers can use permission systems provided by the OS for access to features that often correspond in practice to terminal access requiring consent.
  - The developer should analyse the permission systems provided to determine whether or not they alone allow consent to be obtained in accordance with the criteria set out in the texts. In particular, the consent screen must show the purpose for which permission is required, and must be able to provide a link to a document containing all the information provided for in Articles 13 and 14 of the GDPR. Otherwise, it is necessary to implement a *Consent Management Platform*

(CMP) in addition to the permission window (e.g. to allow complete information or to ensure granularity of consent).

- The developer should ensure that the use of these additional collections of consent does not create confusion among users, especially when the refusal associated with a permission actually expresses the will to oppose the use of tracers. In this case, the consent given through the CMP following a refusal expressed during a request for permission cannot be considered unambiguous, and thus will not be valid under the regulations (for example, consent granted in a broad CMP, including the possible collection of geolocation, followed by a refusal of permission to collect geolocation system).

6.3. Making good use of SDKs

In practice, the developer chooses the SDKs that they offer to the publisher, who is responsible for the final integration decision within the application. It is strongly recommended that the developer implement in this context a rigorous approach to selecting and implementing the SDKs he intends to use.

1. Select SDK according to the right criteria

Before any proposal for the integration of an SDK, it is recommended that the developer, when studying the tools he wishes to implement, follow a privacy-based assessment methodology.

- **What documents should I ask the SDK provider?**
  - Documents making it possible to determine all the data processing operations involved in the integration of the SDK, for example in the form of a register of processing operations, depending on the settings implemented, so that the controller can integrate it into its own registry.
  - The elements to determine the qualification of the SDK provider for each of the treatments. On the criteria for qualifying the SDK provider, the developer may refer to Part 4 of these recommendations.
  - The identification of any unauthorised transfers or disclosures of personal data (Article 48 GDPR).
- **What analysis should be carried out?**
  - If the developer chooses to propose the integration of an SDK in the development of the application, he should provide the publisher with the elements to perform a qualification of his responsibility and request written approval before the SDK is integrated. Indeed, if it acts as a processor and a processing involves the use of a sub-processor, the developer must, in accordance withArticle 28 of the GDPR, obtain the authorisation of the controller and ensure that the same data protection obligations incumbent on that subprocessor are imposed on that subprocessor in a contract or other legal act. Even in the event that the developer is not subcontractor, it is necessary that the publisher is informed and a subcontract will in principle have to link directly the publisher of the application and the provider of the SDK.
  - The developer should ensure that the SDK presents ways to block any processing or access to data stored on the terminal or implement permission until valid consent can be obtained where necessary (see section 6.3.2 “Manage User Consent” below).
  - The developer should ensure that the SDK responds to requests for the exercise of rights, including the right to withdraw consent. SDKs providing APIs to respond automatically should be preferred.
  - These recommendations also apply to SDKs provided by OS providers or those that are offered by default in Apple and Google documentation, respectively for iOS and Android.

Point of attention

Beware of the “Russian dolls” effect, according to which the integration of an SDK involves that of other SDKs. In this case, the analysis should be repeated for each subsequent SDK.

2. Manage User Consent

When choosing an SDK, it is necessary to study the ability of the proposed solutions to allow the proper collection of consent from users when they use tracers requiring consent within the

meaning ofArticle 82 of the Data Protection Act or the realisation as a subcontractor of purposes based on the legal basis of consent.

- **What safeguards are available to enable users to obtain valid consent?**
  - The developer should ensure that the SDK configuration allows this consent to be given prior to any consent-based processing or any read and/or write operation from the SDK. In particular, any reading and/or writing operation within the meaning ofArticle 82 of the Data Protection Act not exempted from consent and which would be carried out at the first launch of the application is to be prohibited.
  - The developer should only offer SDKs allowing the withdrawal of consent.
  - In cases where the selected SDKs claim that they allow for lawful collection of consent, this obligation should be contractually formulated and its compliance audited (see the proposed methodology below).

- **How to ensure the granularity of consent to SDKs?**
  - If several purposes are pursued by the SDK, the developer should ensure that the SDK allows for a granularity of consent, which is generally necessary to ensure that consent is given freely. This means that if consent is obtained for a single purpose, the operations to be carried out by this SDK will have to be limited to that single purpose. If several technical operations contribute to the same purpose, the triggering of such operations may result from a single consent (e.g. in the case of online advertising, the selection of the advertisement and the measure of audience of that advertisement may result from a single consent).
  - The developer should only offer SDKs that technically allow the suspension of their own executions until they have received a signal from the application indicating which executions can be implemented according to the appropriate purposes.

3. Auditing the proper functioning of SDKs

Beyond the collection of contractual and documentary elements, it is recommended that the developer implement sufficient means, and adapted to the technical complexity of the process, to verify compliance with the commitments of the SDKs that he proposes.

- **How can I verify compliance with the commitments made by the SDK?**
  - An audit methodology by interception of network communications should be considered.
  - The developer should at least ensure, as far as possible, that the following points are verified:
    - The SDK does not carry out any reading and/or writing operations (not exempted) prior to the collection of consent;
    - In case of consent for different purposes, the SDK shall respect the choices expressed by the person;
    - The SDK does not collect more data than defined in the provided register;
    - The SDK does not access protected resources when allowing access to them for other functionalities;
    - The SDK respects the withdrawal of consent.
  - The publisher of the SDK, as a subcontractor or subcontractor, is obliged to facilitate the conduct of such audits.
  - In case of SDK evolution, these analyses should be updated.
  - Due to the great complexity of certain application bricks, these arrangements cannot allow them to ensure compliance with the obligations and are only a complement to organisational measures.

6.4. Ensure the security of the application

The security of the processing operations is an obligation of the developer processing data on behalf of the publisher, in accordance withArticle 28 of the GDPR. The developer must, if qualified as a subcontractor, implement all relevant measures for this purpose and at least all the measures required underArticle 32 GDPR.

1. Implement minimum security measures

Among the security measures to be implemented, some can be systematically implemented by the developer.

- **What basic measures is recommended to implement?**
  - Securing communications with servers by systematically encapsulating them in a TLS channel, whose cryptographic sequences are explicitly fixed, in accordance with the ANSSI TLS guide[33];
  - Storage of cryptographic secrets by packaging using APIs allowing the use of cryptographic suites included in the phone, favouring hardware protections such as *Android's Hardware* Keystore or Apple*'s Secure Enclave*;
  - Regardless of the personal data concerned, account should be taken of the possibility of the AOS carrying out automatic backups thereof. Disabling unwanted backups or encryption of data without including the encryption key in them;
  - Where authentication is necessary, use a means of authentication corresponding to the level of security sought (e.g. if a person is to be authenticated with certainty, do not use biometric authentication if the device used allows the registration of biometric templates of different persons);
  - In general, compliance with levels L1 and L2 of the recommendations produced by OWASP[34].

2. Adopt an adequate safety model

In order to implement the relevant measures, it is essential that the chosen security model corresponds to the context of mobile applications.

- **On what principles is it recommended that your safety model be based?**
  - In the general case, the developer should avoid basing his security model on the integrity of the terminal, except in certain justified cases. For example, in the case of banking applications, it may be justified to try to attest to the integrity of the device, to avoid malicious access to passwords. In this case, only the lack of integrity should be reported, without causing a blockage.
  - Similarly, certificate pinning *or* code obfuscation measures are not relevant security measures.
  - The service should be designed to maintain the level of security even with corrupt terminals. Best practices in terms of APIs[35] should be applied to secure the servers used by the application and protect them from potential abuse attempts.
  - The developer should protect personal data against possible unauthorised access by subsequent processors and implement logised access controls to avoid internal diversion.

[33] *" OWASP MAS checklist"*, mas.owasp.org
[34] 'Closed] API: the CNIL submits for public consultation a draft technical recommendation', cnil.fr
[35] 'Attack chain on service providers and design offices: a new threat analysis report', ssi.gouv.fr

3. Ensure the maintenance of security over time

The security of an application cannot be considered only at the time of its first publication but must on the contrary be based on sustainable measures.

- **What measures are recommended to ensure safety over time?**
  - The developer should implement deployment processes that ensure the quality of distributed applications is maintained:
    - adopting a Continuous Integration Deployment and Continuous Deployment (IC/CD) methodology to allow frequent updates of applications, in particular in the case of security updates;
    - securing code deployment with a prior peer review phase.
  - The developer should maintain vigilance regarding the external elements embedded in the applications:
    - ensuring that the versions used are the latest;
    - ensuring that there is no malicious evolution in the SDKs implemented, or libraries used through *supply chain security* [36]practices. To minimise the possible attack surface, using at least elements provided by third parties.
  - The developer should ensure that the versions available on app stores are updated so as not to endanger users:
    - by checking whether it is necessary to impose recent versions of OS, depending on the sensitivity of the data processed. And, if that choice is made, leaving only versions with a minimum data protection risk available as a remainder (last version of an application available for a given version of the OS);
    - by analysing, depending on the security issues encountered, whether it is necessary to force the update of the applications, for example by blocking certain features at the server level for insecure versions of the application.
  - If a personal data breach is proven or even suspected, the developer must notify the publisher as soon as possible so that it can, if necessary, notify that breach, underArticle 28 of the GDPR.
  - The developer should follow the best practices for compliance and security of IT developments, as set out in the GDPR Guide of the development team.

[36] Guidelines 07/2020 on the concepts of controller and processor within the meaning of the GDPR (PDF, 1.6 MB), edpb.europa.eu

6.5. Checklist

Category	Sub-Category	Identifier	Description
Formalise its interaction with the publisher	Identify the responsibilities and duties of each person	1.1.1	A register of processing operations including the qualification of each of the participating actors is provided during the contractualisation.
		1.1.2	The conditions for the implementation of each treatment are clearly stipulated in the contract.
		1.1.3	A contact point at the publisher is designated for the validation of any choice impacting the processing of personal data.
		1.1.4	A register of the processing operations actually implemented is kept and made available to the publisher, and in case of discrepancy, the latter is alerted.
		1.1.5	The developer's obligations (in particular Articles 28 and 30.2 GDPR) are identified and implemented.
	Implement project management processes approved by both parties	1.2.1	Any decision affecting the privacy of users is validated by the publisher in writing, after information and advice from the developer.
		1.2.2	A process of monitoring external developments that may impact the processing is implemented, which includes the editor's alert.
		1.2.3	All the elements necessary for the correct information of the people are transmitted by the publisher in case of delegation of the publication in the application stores.
	Identify all treatments	1.3.1	The treatments implemented by the OS through the use of functionalities that it makes available are identified and validated by the publisher.
		1.3.2	The treatments implemented following the integration of SDKs are identified and validated by the publisher.
Assume its role of advising the publisher	Propose developments respecting the principles of protection of personal data	2.1.1	Technical solutions at the state of the art are analysed and proposed to the publisher to minimise the collection and limit the impact of making the data available to third parties.
		2.1.2	The least intrusive permission is chosen for each data collected through this system, and it is only triggered when it is needed.
		2.1.3	Sensitive data (within the meaning of Article 9 GDPR) are distinguished from

			other types of data, in particular in terms of architecture.
		2.1.4	Sensitive data is not made accessible to third parties (e.g. SDKs).
	Help to ensure that users' rights are respected	2.2.1	A mobile-readable privacy policy is provided by the publisher and integrated within the application, in an accessible manner.
		2.2.2	The exercise of rights is possible simply, for example by means of a page embedded in the application.
		2.2.3	The exercise of rights includes all processing carried out within the application, including those carried out by third parties such as SDKs.
	Participate in compliance with the use of tracers and the collection of consent	2.3.1	The operations covered by the need for consent are identified and specific written instructions are requested from the publisher on this matter.
		2.3.2	The consents obtained meet the requirements described in the recommendation " *Cookies* and other tracers", adapted to improve readability on mobile devices.
		2.3.3	If the same operation is subject to consent and permission, the articulation between these elements is not likely to create confusion among users.
Making good use of SDKs	Select SDK according to the right criteria	3.1.1	Documents to determine all the processing and data collected during the integration of the SDK shall be made available by the SDK provider.
		3.1.2	The responsibilities are qualified for each of the treatments implemented as part of the SDK integration, and validated by the publisher.
		3.1.3	The SDK respects the user's consent and responds to requests for the exercise of rights.
	Manage User Consent	3.2.1	The SDK shall provide information to ensure the correct information on the purposes pursued when obtaining consent.
		3.2.2	SDK allows granularity and withdrawal of consent.
		3.2.3	The SDK does not read and/or write before consent (in particular at the first launch of the application).
	Auditing the proper functioning of SDKs	3.4.1	Compliance with the commitments made by the SDK provider is audited, with the latter's assistance.

Ensure the security of the application	Implement minimum security measures	4.1.1	Communications are systematically encapsulated in a TLS channel.
		4.1.2	The cryptographic suites of the OS are used, as well as the hardware protections of secrets.
		4.1.3	Backups (especially automatic) are encrypted with a local key.
		4.1.4	Levels L1 and L2 of OWASP MAS are achieved.
	Adopt an adequate safety model	4.2.1	The security model is not based on the integrity of the terminal.
		4.2.2	Any integrity defect detection is indicated to the user and not used to block the user.
		4.2.3	APIs incorporate elements to secure services.
		4.2.4	Personal data are protected against possible internal diversion or by subcontractors.
	Ensure the maintenance of security over time	4.3.1	The application is updated as often as necessary in terms of security.
		4.3.2	Any malicious evolutions of SDKs or libraries used are monitored in the context of *supply-chain security* practices.
		4.3.3	The application is updated in the event of the evolution of the OS following security breaches, depending on the sensitivity of the treatments.
		4.3.4	Any suspected or proven personal data breach is reported to the publisher.

7. SDK provider-specific recommendations

Package leaflet

Who are these recommendations addressed to?

- These recommendations are addressed to **providers of software development kits (or SDKs for *software development kits*)**.
- The SDK provider is defined as **the legal entity that makes available one or more SDKs intended to be integrated into mobile applications,** often involving processing servers, accompanied by documentation relating to their integration with third parties**.**
- In practice, these recommendations are specifically addressed within the SDK provider:
  - the *Data Protection Officer (DPD)*of the SDK's publishing entity;
  - technical teams in charge of developing and maintaining the SDK;
  - teams responsible for commercial relations with partners (developers or publishers), to facilitate integration and contractually frame it.
- These recommendations can also be consulted by other players in the mobile ecosystem such as app publishers and developers, app store providers or operating system providers.

What is the purpose of these recommendations?

- These recommendations concern SDK providers processing personal data, as part of the implementation of SDK by mobile applications that integrate it. This data may be processed by the provider on its own account, on behalf of the publisher of the mobile application, or jointly by both actors. It is therefore essential that in these different configurations the respective roles and qualifications of each actor with regard to the processing of personal data are previously identified.
- Nevertheless, there are also SDKs that are intended to be integrated into mobile applications and offer only local features, or do not lead to remote processing. As such, their suppliers act solely as software providers and do not necessarily have a qualification within the meaning of the GDPR due to their failure to implement personal data processing. However, they are encouraged to ensure that the design and architecture of the software they provide does not hinder or complicate compliance with the GDPR by the controller who will use it, and to follow the best practices highlighted in these recommendations.

How to use these recommendations?

- These recommendations are organised into several sections, each corresponding to a step in the provision of an SDK by a provider. Each party outlines privacy issues and brings together a series of recommendations and best practices to implement.
- A **consolidated checklist of key recommendations** for KKD providers is proposed at the end of this section. SDK providers are invited to study this list and use it in particular when drafting their contractual documentation.

See also

SDK providers are also invited to consult the recommendations applicable to other actors, which may affect them incidentally, and in particular the following:

- Publisher-specific recommendations
- Developer-specific recommendations

7.1. Design your service

Privacy considerations should begin at the design stage of the SDKs made available to application publishers, where appropriate through their developers.

1. Identify and analyse its obligations under the applicable regulations on the protection of personal data

It is important to determine precisely the obligations of the SDK provider according to its qualification.

- **What qualifications for the treatments implemented?**
  - As part of the provision of SDK, different qualifications are possible depending on the specificities of the processing of personal data involved.
  - The SDK provider may refer to Part 4 of these recommendations to characterise all the treatments that it is likely to implement in the provision of SDKs. In particular, it is possible to qualify as a processor or as a joint controller in the light of the criteria laid down in the European Data Protection Board (EDPS) Guidelines 07/20[37].
  - Some recommendations specific to other actors may be applicable to SDK providers in some cases, depending on their qualification for each treatment.

- **What specific points of attention?**
  - The SDK provider should identify whether the data collected constitutes sensitive data within the meaning of Article 9 GDPR (see box below).
  - More generally, it should avoid, in their design, that the tools it proposes collect personal data; if this collection is indispensable, it must never be produced without the knowledge of the persons concerned.
  - If the SDK provider is a controller or joint controller, it should pay particular attention to ensuring that data subjects are informed (see part 4 of these recommendations).
  - If the SDK uses tracers (including through the implementation of a read or write operation on the user's terminal, e.g. a software or hardware identifier), this use should be precisely analysed, depending on the qualification and responsibilities of the SDK provider, referring in particular to Part 6 of this Recommendation ('Developer Specific Recommendations').
  - The SDK provider should also ensure that its customers are aware of the place of storage of the data, insofar as contractual and/or technical supervision of data transfers within the meaning of Chapter V of the GDPR[38] may be necessary[39].

What is sensitive data within the meaning of Article 9 GDPR?

- **See Part 5.1 of these recommendations:** " Ensure the legal conformity of processing operations"

[37] "Transfer of data outside the EU", cnil.fr

[38] See in this regard EDPS Guidelines 01/2020 on measures that complement transfer instruments to ensure compliance with the level of protection of EU personal data (PDF, 389 KB), edpb.europa.eu

[39] See in this regard Decision No SAN-2019-001 of 21 Jan. 2019 of the CNIL.

2. Apply data protection principles by design and by default

It is recommended, for each of the treatments envisaged and according to the qualification within the meaning of the GDPR and the responsibilities of the SDK provider, to analyse whether personal data protection measures by design and by default may apply.

- **How to minimise the data collected?**
  - The principle of minimisation must, in particular, lead to limiting data sent to servers (such as those of the SDK provider, like those of its partners) to the strictly necessary, in the light of the purposes pursued, to the strictly necessary in order to achieve the purpose of the processing.
  - Default configurations of SDKs that comply with this principle should be proposed, including in the configuration examples offered in its documentation.
  - In particular, the collection and registration of terminal, network (IP address, surrounding network hardware) or individual identifiers should be avoided if the use of SDK does not require it.
  - Where the OS provider or a third party service offers a more privacy-protective functionality to process certain information (e.g. rough geolocation instead of fine geolocation), which seems more relevant in terms of data minimisation, this should be implemented and partners should be informed of the need to update their SDK to take this into account.
- **How to partition the different services?**
  - It is recommended that the SDK provider design its service from the outset so that its functionalities can be decorated with each other and thus allow a simple configuration of the different options, especially if the processing of these different options involves different responsibilities.
  - For example, if the SDK provider provides audience qualification services (as a subcontractor) but also data collection services for retargeting for its own account (as controller), independent selection of these two features by the publisher should be allowed for SDK integration, possibly with a paid alternative if this choice impacts the SDK provider's business model. If these features require consent, this technical decorrelation may also be necessary to meet the need for user consent.
  - In the same vein, the SDK provider should avoid as much as possible grouping all the services and features offered within the same SDK, in order to allow the publisher to use only the SDK that is useful to it. Alternatively, the SDK can be designed in a modular way, so that only the elements corresponding to the functionalities actually used are integrated into the application, which helps to limit the presence of possible vulnerabilities.
- **What system permissions for which treatments?**
  - When designing, the SDK provider should analyse useful system permissions, distinguishing between those that are strictly necessary and those that are desired but not indispensable, as they simplify the user experience but are not essential to the desired functionality. For example, a conversational wizard module may want to have a voice input, which requires mic access permissions, but should not make this request systematic.
  - The provider should be careful to choose the least intrusive level of permission possible, or to propose different configurations at the user's choice.
  - The SDK provider must also clearly distinguish between permissions for service rendered to the application of subsequent permissions and processing of data that it performs on its own account and which are sometimes linked to its business model.
  - It should ensure that the SDK is as little dependent as possible on obtaining permissions, in particular by studying the use of alternatives as set out in Part 5.5 of these recommendations ('Permissions and data protection by design'),

whether these alternatives are by hand by direct users (publishers or developers) or by the user of the application.

7.2. Document the right information

While the responsibility for compliance with the GDPR of a significant part of the processing implemented in the application lies with its publisher, the processing generated by the integration of SDK can significantly impact the work of these publishers in the information they communicate and the analysis of the treatments implemented. It is therefore the responsibility of the SDK provider to document the information necessary to demonstrate the correct application of the texts.

1. Identify the information to gather

It is important for the SDK provider to ensure that all the information necessary to comply with its obligations and/or those of its partners is documented.

- **What information should be provided on the processing operations carried out?**
  - Regardless of the operations of an SDK offered by SDK providers, it is important that its provider prepares and makes available to its customers a clear analysis of the treatments involved in the use of the SDK, and that the provider simply provides the software or plays an operational role in the actual implementation of the treatments.
  - For the processing in which the SDK provider will have a responsibility within the meaning of the GDPR:
    - the SDK provider must maintain and maintain its own register of processing activities, according to its qualification within the meaning of the GDPR and in accordance withArticle 30 GDPR;
    - for each processing, he must identify, if necessary with his partners, the qualification which falls to him within the meaning of the GDPR.
  - If it acts as a processor and a processing involves the use of a third-party subprocessor, it must, in accordance withArticle 28 of the GDPR, obtain the authorisation of the controller and ensure that the same data protection obligations incumbent on it under the contract with the controller are imposed on that subprocessor, by contract or any other legal act.
- **What information should be provided on the use of tracers?**
  - The SDK provider must inform its partners precisely about the trackers used that implement read and/or write operations on the user's terminal (for this purpose, he can refer to the developer-specific recommendations for identifying these occurrences).
  - It must indicate the purposes pursued by each of these uses of tracers, or the functionalities that they allow.
- **What information on permissions should be documented?**
  - The SDK provider must inform its partners of the permissions required by the SDK
  - For each permission requested, it must indicate in particular whether it is associated with a reading and/or writing operation within the meaning ofArticle 82 of the Data Protection Act, which may require specific consent from the user.
  - It must specify the optional or mandatory nature of these operations according to the proposed functionalities.

2. Present this information in an accessible format

This information is ideally made available in an accessible format and a formalism facilitating its analysis, regardless of the settings relating to the treatments implemented.

- **What arrangements for making available?**
  - The SDK provider must ensure that the necessary information (mentioned above) is up-to-date and easily accessible by all its partners, in order to enable them to meet their own obligations.
  - Some of this information, in particular as regards the respective qualifications and obligations of the parties within the meaning of the GDPR and the collection of possible consents, must be formalised in the contractual documentation.
  - Any evolution of the service affecting privacy issues must be made available to and expressly indicated to the partners of the SDK provider. If the SDK provider is a processor, these developments must also be approved by the controller prior to their implementation.
- **What formalism should I adopt?**
  - Where the SDK provider is a controller or processor, the SDK provider must keep a record of processing including all the information referred to in Article 30 GDPR:
    - This register must separate each of the processing operations carried out, a processing being defined by its purpose. If treatments depend on the parameters chosen, it is advisable to provide partners with a dynamic register according to the settings of each client. Otherwise, the parameters for each treatment should be carefully indicated so that partners can easily understand which treatments are being implemented as part of their particular configuration.
    - For each processing, the data collected for each processing should be clearly indicated. To facilitate reading and analysis, it is recommended to choose a format that allows easy handling of information, for example via a spreadsheet file (which makes it easy to identify all the processing related to a data).
    - For each processing operation, it is also mandatory to indicate the legal basis identified and the obligations arising therefrom.
    - The register should be designed in such a way that it can extract relevant information for the partners of the SDK provider, identifying in particular what is business secrecy.
  - Similarly, when the SDK provider is responsible or jointly responsible for processing these operations, the SDK provider must document the reading and/or writing operations it implements. It may present this information in an easily readable table:
    - indicating, for each line, the operation carried out, the associated permission, the purposes pursued (and potentially the corresponding registry line) and the technical means of blocking or activating this reading (to facilitate the implementation of consent management tools by the partners);
    - proposing, for each line, examples of formulations that can be used by the controller to inform users when collecting consents;
    - Documenting the SDK versions that use each line, to allow partners to choose the appropriate version and understand the effects of a possible SDK update they have integrated.

7.3. Managing people's consent and rights

As a subcontractor, the SDK provider can have a strong impact on the respect of the rights of individuals, in particular by facilitating the exercise of rights, but also by designing mechanisms to facilitate the collection of consent.

1. Assist in the proper exercise of users' rights

When subject to the GDPR, and according to its qualification, the SDK provider is obliged to respond directly to requests for the exercise of rights (as controller), or to assist the controller in responding to them (as a processor).

- **How to ensure that data subjects are informed about the processing of personal data related to the SDK?**
  - If the SDK provider is a controller or joint controller, it is the responsibility of the SDK provider to ensure that individuals are informed. Since the SDK is intended to be integrated into a mobile application that depends on a publisher, this information will generally have to be integrated into the information provided by the publisher to the user.
  - He can take care of this by contractually requiring the publisher or developer who uses his services to proceed with this information.
  - The same applies if consent is required for the processing for which the SDK provider is responsible.
  - Where applicable, the SDK provider may propose an interface software component (CMP type) that can also be integrated into the application and allowing the collection of the user's consent for these purposes.
- **How to ensure that users can easily exercise their rights?**
  - The exercise of rights may concern processing under the responsibility of the publisher of the application and the role of the SDK provider, if it is a subcontractor, is then a compliance support role, which depends on the functions entrusted to it under contract. It may also concern processing under the own responsibility of the SDK provider, which is then fully in charge of ensuring compliance with the rights opened to individuals by the GDPR.
  - The exercise of rights must be considered from the outset, in particular in terms of the structuring of databases. The right of deletion, in particular, must be able to be respected independently of technical constraints.
  - To facilitate the practical implementation of the exercise of rights, the possibility of automating it should be analysed, in particular by means of APIs that can be integrated within applications or at the client server level.
  - In this case, the SDK provider should ensure that as few additional identifiers as possible are used to process the exercise of these rights. For example, if data are associated with the person simply on the basis of an advertising identifier, it should be sufficient to enable the exercise of human rights. Conversely and in the light of Article 11 GDPR, in the context of mobile applications, a request for the exercise of rights may not be able to receive an effective response. For example, in the event that the person has reset his/her advertising ID and no longer has knowledge of the previous identifier(s), an additional collection of information would then be necessary to re-identify the person.

2. Participate in compliance with the use of tracers and the collection of consent

If the qualification of the SDK provider is that of a processor within the meaning of the GDPR, assistance to the controller implies advising the controller, in particular on the possible need to obtain consent, to provide the technical means to enable it to be properly taken into account, as well as its withdrawal. The cases in which consent is required either under Article 82 of the

Data Protection Act or under the GDPR are recalled in part 5.1 of these recommendations: 'Ensure the legal conformity of the processing operations'.

- **Can the user's permissions for the application be used to obtain consent to the processing carried out by the SDK?**
  - When access to a terminal resource through the application requires the consent of the user, it is necessary to ensure that valid consent has been obtained for each purpose pursued.
  - As a result, the SDK's access to a protected resource and the resulting processing, if they require consent, cannot systematically be carried out solely on the basis of permission granted to the application. In particular, if permission is granted to the application for a purpose distinct from that of the SDK, it is not possible to consider that this permission can be used for the SDK without a new consent of the data subject.

- **How to allow a valid collection of consent?**
  - Technical and organisational means to block any processing or access to data stored on the terminal (or system permissions permitting it) should be offered, until valid consent is obtained. Specifically, this means that the provider should allow its SDK to be able to suspend its execution until consent has been provided.
  - For consent to be valid, it must be given in a specific way (distinguished in particular from the acceptance of the terms of use of the application) and free (which in principle implies being able to choose to grant or refuse consent according to the different types of purpose).
  - As such, if the processing pursues several separate purposes, the signals relating to the consent of the user must be taken into account in their granularity, purpose by purpose, regardless of the status of the requested permissions.
  - For each of the consents sought, the design and documentation of the SDK should provide for the possibility and anticipate the functional impacts of a user's lack of consent to the user, in order to minimise any unnecessary blockage of functionality in the event of refusal.
  - The revocation of consent for these purposes must be properly taken into account after it has been initially granted. In particular, the SDK provider should ensure that the revocation does not lead to instability in the execution of the application or cause a constant request for the revoked permission, which would call into question the freedom of consent.

- **What best practices should be implemented?**
  - The SDK provider should ensure that the use of installation *-time permissions is minimised by preferring the use of triggerable permissions* during the operation of the application (' *runtime permissions*'), in order to facilitate the possible integration with the application editor's collection tools and, where justified, in order to contextualise requests for consent. Thus, if the feature in question is never used, the relative permission should not be displayed.

7.4. Participate in maintaining compliance of the application over time

The SDK provider shall, when qualified as a subcontractor, participate in the implementation and maintenance of compliance of the application over time, by providing secure elements, but also by accompanying the compliance of applications that use its products.

1. Offer secure SDKs

As a processor within the meaning of the GDPR, the SDK provider is subject to the same security requirements as other actors providing executables, such as the external developer of an application. Even in cases where the SDK provider is simple software provider, it is encouraged to follow these recommendations.

- **What security measures should be implemented?**
  - See recommendations in part 6.4 of these recommendations: 'Ensure the security of the application'.

2. Allow audits to be carried out

Where the qualification of the SDK provider within the meaning of the GDPR is that of a subcontractor, the latter is obliged to contribute to the performance of audits (Article 28.3.h GDPR).

- **How can audits be facilitated?**
  - It is the responsibility of the SDK provider, in addition to providing clear information and up-to-date technical documentation (see above) in accordance withArticle 28, to facilitate the conduct of audits, including in an operational manner.
  - As such, the SDK provider and its subcontractors may have to answer specific questions about the treatments implemented.
  - These questions may follow the mere diligence of their client or be transmitted as part of a control by a European data protection authority or following the receipt of a complaint or a complaint about one or more specific processing operations of an application related to the operation of the SDK.
  - The SDK provider should, as far as possible, allow for the transmission and obtaining of responses to them.
  - It is recommended that the SDK provider, on a regular basis and at its own initiative, carry out audits on its SDK in order to anticipate and prevent problems that may subsequently be identified by its partners or supervisory authorities.

3. Implement robust processes in terms of compliance

The maintenance of SDK compliance should be designed over time, with processes to update in line with changing implementation conditions.

- **What measures are in place to ensure safety over time?**
  - Vulnerability reporting tools and methodologies, in the event of proven exploitation of vulnerability, should be put in place. As a processor, the SDK provider is obliged to inform its controller in such a way as to enable it to comply with its obligations with regard to the security of personal data (Articles 32 to 36 GDPR).
  - In the event of a personal data breach within the meaning of the definition ofArticle 4 GDPR and depending on whether the SDK provider is responsible or joint controller for each processing carried out by its SDK, it may also have to notify the data breach itself to the authority of the country to which the entity depends, as well as possibly to the data subjects (Articles 33 and 34 GDPR).
- **How to take into account possible developments in its partners?**
  - It is the responsibility of the SDK provider to monitor changes in the data privacy policies of the partners, to ensure that the treatments mentioned in them

correspond to the treatments actually implemented. If he finds that information is missing or too general, it is his responsibility to report it to his partner.

- The SDK provider should also monitor the technical developments of APIs offered by operating systems. Updates to the OS often lead to changes in the functioning of certain methods, which can have an impact on privacy. The provider should update its SDK in the light of technical developments in the OS.
- In particular, the SDK provider should consider whether these developments can make it possible to implement the processing in a privacy-friendly way by design. If so, it should update and encourage the use of the latest versions of its tool.

7.5. Checklist

Category	Sub-Category	Identifier	Description
Design your service	Identify and analyse its obligations under the applicable regulations on the protection of personal data	1.1.1	A qualification within the meaning of the GDPR (controller, joint controller or processor) is defined for each processing of personal data carried out by the SDK.
		1.1.2	Sensitive data (within the meaning of Article 9 GDPR) are identified and their processing modified accordingly.
		1.1.3	The default configuration of the SDK allows the application that uses it to avoid unintended or excessive data collection.
		1.1.4	Any readings or writings performed by the SDK are defined and documentation is made available to third-party developers.
	Apply data protection principles by design and by default	1.2.1	The data collected by the SDK as well as those transmitted to the partners are minimised, so as to strictly limit the purposes defined by the controller.
		1.2.2	The different features offered by the SDK can be integrated and executed in a decorative way, especially if they do not all involve the same responsibilities or purposes.
		1.2.3	If it is not technically possible to decorate the features of the same SDK, these are split into several separate SDKs.
		1.2.4	The permissions required for the execution of the SDK are minimised, distinguishing those strictly necessary from those desired but not indispensable.
		1.2.5	When several permissions can allow the collection of data in its desired form, the choice is made over those with the least intrusive technical capabilities.

Document the right information	Identify the information to gather	2.1.1	A clear analysis of the treatments driven by the use of SDK is carried out and accessible.
		2.1.2	An SDK-specific processing record is maintained and maintained.
		2.1.3	The register indicates for each processing the qualification of the actors, within the meaning of the GDPR.
		2.1.4	For each processing involving the use of a subprocessor, the list of data collected is drawn up, the purpose analysis is carried out and the authorisation of the controller is obtained.
		2.1.5	The presence of tracers implementing reading or writing on the end-user's terminal is indicated precisely.
		2.1.6	The optional or mandatory character for each of the permissions required by the SDK is indicated, depending on the functionality used.
	Present this information in an accessible format	2.2.1	The above documentation and information are up-to-date.
		2.2.2	The above-mentioned information is formalised in the contractual documentation when it needs to be.
		2.2.3	Specific information is provided when SDK updates involve an evolution of the treatments implemented, allowing third-party partners to analyse over time what impacts them.
		2.2.4	When these modified processing operations are operated as a subcontractor, the collection of their authorisation shall be carried out again with the publisher, prior to their implementation.
		2.2.5	The processing register clearly distinguishes the purposes associated with each processing.
		2.2.6	If the purposes pursued depend on the setting of the SDK, a dynamic or separate register is made available, depending on the possibilities of setting the SDK, so that the controller can easily integrate the elements of the registry that correspond to its setting in its own processing register.
		2.2.7	The format of the register, for example in the form of a table, makes it possible to easily and exhaustively identify each data collected, as well as the legal (legal basis, purpose, obligations) and technical elements (reading, entries) associated.

		2.2.8	Examples of wording relating to the processing carried out are directly proposed, so that a third party partner can easily reuse them for their own collection of consents.
Managing people's consent and rights	Assist in the proper exercise of users' rights	3.1.1	APIs are made available to third-party partners, when they receive requests for exercise of rights, so that these requests can be automatically reflected in the SDK's technical infrastructures.
		3.1.2	The implementation of these APIs does not, or as little as possible, use additional identifiers, so that these rights requests can receive an effective response.
	Participate in compliance in terms of the use of tracers and the collection of consent	3.2.1	A consent check is performed by the SDK where necessary, whether access to the end-user's own resource is performed on behalf of the SDK or on the third party partner account, so that access to a system permission is not technically sufficient for the SDK to collect data.
		3.2.2	The necessary system permissions are granted in the contexts of use where they are necessary for the execution of the intended processing.
		3.2.3	The SDK is technically designed to allow a suspension of its execution until valid consent, by purpose, is obtained.
		3.2.4	If more than one purpose is pursued, the SDK technically allows a separate signal to be taken into account by purpose, always independently of system permissions.
		3.2.5	Alternatives are offered to third-party partners in the event of a refusal by the end user, in order not to alter the proper execution of the application integrating the SDK.
		3.2.6	Revocation of consent does not alter the proper execution of the third party partner's application, both functionally and vis-à-vis the user experience (such as a request for consent displayed in a loop).
		3.2.7	System permission requests are made during the execution of the application rather than when it is installed, where possible.
Participate in maintaining compliance over	Offer secure SDKs	4.1.1	Communications are systematically encapsulated in a TLS channel.
		4.1.2	The cryptographic suites of the OS are

			used, as well as the hardware protections of secrets.
		4.1.3	Levels L1 and L2 of OWASP MAS are achieved.
		4.1.4	The security model is not based on the integrity of the terminal.
		4.1.5	Any integrity defect detection is indicated to the end user and not used to block the end user.
		4.1.6	The security of the service is made effective by securing APIs.
		4.1.7	Personal data is protected against possible internal diversion or by subcontractors or sub-processors.
		4.1.8	Any suspected or proven personal data breach is reported to the partner publisher or developer, whether they are controllers or joint controllers.
time	Allow audits to be carried out	4.2.1	Audit reports are carried out on a regular basis and are made available to partner publishers and data protection authorities upon request.
	Implement robust processes in terms of compliance	4.3.1	A technical and organisational process relating to possible data breaches is established, which provides for the transmission of information to the controllers as well as the formalism of notifications of breaches to the data protection authorities.
		4.3.2	Regular monitoring is applied on the privacy policies of the partners, in order to be able to assist them and inform them if these policies did not correspond to the treatments implemented by the SDK.
		4.3.3	Regular monitoring shall be applied on the technical developments of mobile operating systems and the APIs they make available, in order to strengthen the principles of protection by design and protection by default, including by accompanying third-party partners.

8. Recommendations specific to the OS provider

Package leaflet

Who are these recommendations addressed to?

- These recommendations are addressed to **operating system providers (or OS, for *operating system*)**.
- In the context of these recommendations, the OS provider is defined **as the legal entity that makes an operating system available on a terminal.**
- This operating system may, depending on the situation:
  - be developed in its entirety by an entity for exclusive use on devices it makes available (e.g. iOS, developed by Apple);
  - be developed in its entirety by an entity for licensed use on devices produced by third parties (e.g. Android, developed by Google);
  - be based on a pre-existing OS whose license allows reuse, which is then modified by an entity (according to a connection process, or " *fork*"), for use on its own devices or for making available to end-users (e.g. LineageOS, based on Android and developed by LineageOS LLC).
- In practice, the target audience for these recommendations includes:
  - data Protection Officers (*DPDs)*;
  - developers and lawyers from the entities that provide these OSs.
- These recommendations can also be consulted by other actors in the mobile ecosystem: app editors and developers, app store providers, software development kits (SDKs), etc.

What is the purpose of these recommendations?

- OS providers, as part of the normal operation of the terminal and applications executed by the user, may be required to process personal data. As such, the functionality of the APIs they provide applications plays a major role in the ability of application publishers to deliver content that complies with applicable data protection rules. It is important that OS providers allow configurations to facilitate application compliance.
- Moreover, in the context of the publication of an OS under a license allowing its reuse, the design choices are likely to be passed on, identically or in a similar form, by all actors reusing the published source code. It is therefore important that good privacy by design practices *can*be *implemented by OS providers so* that all actors in the chain reusing the code can benefit from it and *ultimately* improve the privacy protection of end-users of those OSs.
- Some providers make the choice, regardless of basing their OS on a pre-existing OS, to integrate a set of third-party apps into it. These technological choices involve many data processing that it is important to identify, both by the consequences on individuals and for the legal qualifications that flow from them within the meaning of the GDPR.

How to use these recommendations?

- These recommendations are organised into several sections, each corresponding to a step in the provision of an OS by a manufacturer itself, to other manufacturers or directly to end users. Each party outlines privacy issues and brings together a series of recommendations, as well as good practices to implement.
- These recommendations apply without prejudice to the rules applicable on other legal grounds than the protection of personal data, including competition law.
- A **consolidated checklist ofkey recommendations** for OS providers is proposed at the end of this section. OS providers are invited to study this list and use it in particular when drafting their contractual documentation to ensure, where appropriate, that these recommendations are taken into account by its partners.

8.1. Ensure compliance of the processing of personal data implemented

If this is not its main role in the context of mobile applications, with the OS primarily providing features for application developers, it is possible that some personal data processing may be implemented at its initiative. As such, it is necessary to comply with the obligations relating to such processing.

1. Identify and analyse the compliance of the processing of personal data implemented

The first step is the proper identification of the entities concerned as well as the processing operations actually carried out by those entities.

- **Which entities can participate in the implementation of personal data processing in an OS?**
  - Since the AOS is not necessarily provided in its entirety by a single entity, each provider should conduct an analysis of its responsibilities, which will depend on the actual supply of functional bricks and treatments used by applications and people.
  - This analysis must be carried out when the OS provider determines " *the purposes and means of the processing*" (Article 4.7 GDPR), and is therefore responsible for the processing carried out by an element made available by him.
  - This may be the case, depending on an analysis to be carried out on a case-by-case basis, regardless of the configuration of the OS (see Part 2 of these recommendations 'What professionals are active in the mobile application sector?'):
    - in the case of an entity developing and making available an OS intended to be run (only or predominantly) on its own terminals;
    - in the case of an entity reusing third-party software bricks on its own account, in order to propose a new OS, for example to be used on its own terminals;
    - in the case of an entity developing and making available an OS intended to be run on third-party terminals, provided that such execution implements processing on its own account.

- **What processing of personal data may be concerned?**
  - The question of the processing operations which may be the responsibility of the OS provider is detailed in Part 4 of this Recommendation, in particular 'Qualification of the operating system provider'. In particular, in many cases, the OS is limited to providing software tools without assuming responsibility.
  - The processing operations concerned may be linked to functions implemented in different contexts, for example:
    - the processing of data relating to the use of sensors (e.g. pre-processing of geolocation data);
    - the processing of data relating to the provision of functionalities to applications (e.g. notification services, unannounced termination management, so-called ' *crash*' services, and remote backups);
    - the processing of data specific to the OS (e.g. telemetry and bug reporting).

2. Apply data protection principles by design and by default

For each of the envisaged processing operations, it is recommended to analyse whether data protection measures by design and by default may apply.

- **Is the default setting of the OS the least intrusive possible?**

- The OS provider must verify that no processing carried out on its own account requiring the consent of the user and that no reading or writing on the terminal not exempted from consent occurs before the collection of valid consent under the GDPR and the Data Protection Act.
- It must ensure that this consent is collected in a specific and distinct manner from the validation of the conditions of use of the terminal. Where the purposes for which consent is required are not strictly necessary for the use of the terminal, it must clearly indicate to the user the optional nature of the consent for those purposes.
- It should allow a functional use of the terminal by the user, in particular its default applications or installed by its own means, without the need for an account creation. It must avoid deceptive information schemes (' *dark patterns*') intended to induce him to create an account to use his terminal if this is not necessary[40].

- **How can the data processed by the AOS as controller be minimised?**
  - In some cases, OSs process data as controllers, independently or as part of providing functionality to third parties (e.g. applications) or the user. The measures to be implemented then depend on the treatments carried out.
  - Concerning the transmission of notifications to users of the application:
    - the OS provider should allow the use of third-party notification servers, optimising their use in such a way as to minimise the impact on the terminal's capacity, for example in terms of battery;
    - it should offer developers, to improve the privacy of users' data, up-to-date tools allowing encryption of the data contained in the notifications, regardless of the system in charge of transmitting them. As such, it is recommended to clearly indicate how these tools are used in the documentation for developers.
  - Concerning telemetry and bug lifts:
    - it should propose a bug-removal and *crash* management system that does not involve new data processing, in particular to third parties or to itself: ideally, only the publisher and its subcontractors have access to bug and termination data;
    - it should enable publishers and third parties, including itself, where appropriate, to obtain the collection of consent from users prior to each re-uptake of such data or their transmission to third parties.
  - Concerning remote storage of backups:
    - it should ensure that these are carried out only following an explicit request from the application and not by default;
    - it should allow them to be encrypted, preferably by default, with a key that is not accessible to the OS provider itself.
  - Concerning the pre-processing of geolocation data:
    - the OS provider should allow the location data application, as well as the user, to easily limit the use of geolocation to the GPS sensor data alone, without the need to mobilise other services and sensors such as surrounding Wi-Fi or Bluetooth connections.
    - for the geolocation service based on surrounding connections, a method of calculating the precise location on the terminal and not on the server should be preferred: for example, the terminal can transmit the list of surrounding connections to a server that responds to it by providing it with all the information relating to the connections within a wider perimeter, after which the terminal performs locally the calculation of the precise location on the basis of this precise information.

[40] "Transfer of data outside the EU", cnil.fr

- the OS provider should offer the possibility for the user to be able to easily configure a suspension of the constant collection of geolocation, either by the OS itself or by third parties, so that it is only activated again when it is necessary for a user's use of an application. Thus, a user should be able to choose effortlessly that his geolocation is not collected except when his uses require it, without having to manually activate it beforehand in the OS settings, and then have to return to it to disable it after each use.

8.2. Ensuring that partners are properly informed

OS providers, because of their expertise on the treatments they operate and the features they offer, are best able to provide documentation and advice for the proper use of the features offered. As a good practice, a set of measures can be implemented to this end.

1. Provide comprehensive and clear documentation to support partner compliance

In order to facilitate the proper understanding of the functionalities of the AOS, it is recommended that comprehensive and clear documentation be made available, both technically and legally.

- **To which public should this documentation be addressed?**
  - While it is common for technical documentation to be made available, it may also include elements analysing the specific legislative and normative framework of the European Union, for publishers and developers who wish to target the European market.
  - These legal elements should not be separated from the technical elements, and a common understanding of the impacts of decisions of each type should be fostered to enable joint decisions on the part of those actors.
  - Those elements, and in particular the legal content, should be made available in a language understood by the target audience.
- **What elements include in this documentation?**
  - For publishers targeting the European market, the OS provider should alert in particular to the need to define their responsibility and to put in place compliance measures (finality, information, rights, security, etc.).
  - In addition to the technical elements, it is recommended to incorporate specific guides and tools for DPOs, so that they can integrate them directly into their risk analysis and continuous improvement methodologies.
  - If several development methods coexist functionally, the OS provider should specify the characteristics, both technical and legal, to allow the publisher and developer to make an informed choice taking all of these criteria. In particular, the criteria of backward compatibility, end of support, vulnerability, energy optimisation, deferral of calculation logic, transfers, etc. should be presented.
  - It is recommended to indicate in the official documentation whether the tools made available may or may not meet legal obligations such as collecting consent in accordance with the GDPR criteria (see section 8.3 "Providing tools to enable the rights and consent of users to be respected"), and if so with which configuration.

2. Inform third parties of OS-specific processing

As regards the processing carried out by the OS provider, it is recommended to ensure that third parties are properly informed so that they can meet their obligations, in particular when the use of functionality made available by the OS to the applications leads to processing by the OS.

- **What information should be made available?**
  - The OS provider should ensure that its partners (third party developers and publishers, app stores, builders, etc.) are able to know, understand and document, in accordance with the principle of responsibility, the processing of personal data involved in the use of the OS.
  - In particular, it should indicate, for functions activated by them:
    - the data processed exhaustively for the chosen configuration;
    - the legal qualification, in particular regarding the collection, storage, re-use of data on behalf of the OS provider.
    - specific alert points including greater precision on the involvement of possible transfers within the meaning of Chapter V of the GDPR[41].
- **On which devices to inform third parties?**
  - It is important to provide enhanced information on the devices identified in the previous section (safeguards, notification, telemetry).
  - The OS provider should draw attention to the risks associated with the processing carried out, particularly if they are likely to process sensitive data within the meaning of Article 9 GDPR (see box below).
  - The impact of the settings and default functions of these devices should be clearly explained.

What is sensitive data within the meaning of Article 9 GDPR?

- **See Part 5.1 of these recommendations:** " Ensure the legal conformity of processing operations"

3. Encourage the use of the most protective features

It is recommended that the OS provider make available details of the characteristics of the various functionalities it offers. This should enable publishers to make an informed decision about their use, in order to meet the requirements of personal data protection regulations.

- **How can we encourage the adoption of the most privacy-friendly technologies?**
  - The OS provider should further inform app publishers and developers, over time, about their use of the new APIs offered by OSs:
    - listing the various developments and presenting practical cases;
    - specifying in detail and justified the legal consequences for its partners (effects in terms of compliance, consequences on the publisher's obligations, etc.);
    - by indicating, where appropriate, in a detailed and justified manner, the implementations which comply with the principles of data protection by design and by default (Article 25 GDPR).
  - The OS provider should compile statistics on the prevalence of the use of the most advanced features, and use this information to selectively communicate on the ignored features.
  - It should organise the end of support for the most problematic features, with a sufficient transition period to allow publishers to update their applications.
  - It should organise a dialogue (conferences, research and publications, forums, etc.) with developers, data protection experts and regulators to define priorities for the development of privacy features in the OS.

[41] CNIL, deliberations No 2020- 091 and No 2020-092 of 17 September 2020 adopting guidelines and a recommendation on ' *cookies* and other tracers' respectively. See also "Evolution of web cookie practices: the CNIL assesses the impact of its action plan', cnil.fr.

8.3. Provide tools to enable the rights and consent of users to be respected

While in many cases the OS provider is not involved in the processing of personal data carried out within the applications, the functionalities it provides to app publishers and developers can have an impact on the processes implemented and their compliance. It is therefore important, as a good practice, to put these issues at the heart of its considerations when designing these features.

1. Design of permission systems respecting the principle of data protection by design

The permissions system is at the heart of the protection of users provided by the OS. As such, it is important, when designing it, to implement as many measures as possible to protect the user's personal data. By technically and/or contractually preventing app publishers from accessing certain data, permissions provide a strong technical guarantee of application confidentiality of information, and constitute a major positive measure to safeguard people's privacy.

- **What operations do permissions apply to?**
  - The OS provider should apply user terminal access permissions to its sensors (camera, GPS, environmental sensors), features (network access, Bluetooth, NFC), or storage (contacts, photo gallery, mass storage).
  - It should impose the information and the collection of the user's permission for all of these elements, avoiding hiding permissions from users.
  - It should provide for the collection of an access permission given by the terminal user regardless of the legal obligation to obtain consent under Article 82 of the Data Protection Act for the operation of reading information stored on the terminal.
- **Which scope to choose for permissions?**
  - When a permission is defined, its scope should be analysed under three distinct axes:
    - its degree of precision: each permission can be considered with different levels of precision, to allow the application, or the user, to choose the level of precision strictly necessary for the purpose pursued. For example, in the case of GPS, this data can be made available with different levels of accuracy. Similarly, permissions to access physical sensors (e.g.: barometer, thermometer, photometer, gyroscopes, accelerometer) may sometimes propose a limitation of their accuracy;
    - its material scope: each permission can apply to a larger or lesser set of data or functions. Any permission that is too broad in terms of material scope should be excluded because of the excessive collection of data it causes. For example, any overall permission to access stored files should be excluded, and a file or folder access system should be preferred;
    - its temporal scope: each permission can be activated on an ad hoc basis, or on the contrary for a predetermined duration. Here again, the choice of this scope should be left to the user, possibly accompanied by suggestions of values from the publisher of the application. This temporal scope may also take into account contextual elements, such as the fact that the application is active or not, in the foreground or not, or on the contrary, for a certain period of time.
  - The greatest control should be offered to both the app editor and the user, to restrict the scope of each permission according to these three axes.
- **What additional measures?**

- The OS provider should discourage or even not allow to condition the launch of an application to obtain permissions. On the contrary, it should ensure that applications systematically provide the possibility that the user refuses the requested permissions.
- It should encourage, in particular in documentation and good practices shared with developers, the collection of permissions in a contextual manner, at the time they are needed.
- It should allow users to decline permission without the application being automatically informed of such refusal. For example, it should make it possible to deny access to contacts by returning an empty or partial list of contacts, to localisation by returning random or predefined coordinates manually, etc.
- By default, it should allow users to allow access only once or only when the application is active/foreground/used, especially for the most sensitive permissions. If the application requires permission "at any time" (including when the application is closed), the user's information and consent should be strengthened.
- It should periodically revoke permanent permissions for unused applications, warning the user. It should allow the user to set the frequency of such reminders.
- It should set up an isolation between the execution of the application itself and the execution of SDKs, in a secure manner, to prevent an SDK from benefiting from a permission that would have been granted only to the application, in terms of purposes, consent and information transmitted to the user.

2. Assist in the proper respect of users' rights and consent

By providing tools for this purpose, the OS provider is able to simplify the implementation of proper enforcement of user rights and consent.

- **How can we help with the proper collection of consent?**
  - Although this is not systematic, it is very common for permission requests to correspond to situations in which consent is required, within the meaning of the applicable regulations on the protection of personal data.
  - In order to facilitate application compliance while minimising the fatigue of people's consent, permission windows should directly provide valid consent.
  - To this end, it should be permitted within these windows:
    - specify the purpose for which permission is sought;
    - to integrate hyperlinks to access all the information provided for by the regulations (Articles 13 and 14 of the GDPR, Art. 82 of the Data Protection Act), in particular to the list of lists of third parties involved as controller;
    - to specify the procedures for revoking access.
  - If necessary, and depending on the intrusiveness of permissions, the OS provider should ensure that the user has sufficient information on the impact of their choices. A link to understand this impact could be made available, for example by proposing a series of concrete examples and associated risks. For example, for a terminal SMS access permission, it may be specified that it can legitimately be to retrieve a temporary password as part of multi-factor authentication, but also a time-limited ability for a malicious application to read, transmit or modify received SMS. Such information would be such as to enable the user to estimate the value of that collection and to assess the degree of trust he has in the publisher of an application.
  - The OS provider should also ensure, based on the publisher's instructions that the user is able to understand whether permission is mandatory or optional and the impact of their decision on their access to the application.
  - It should make it easy to revoke or modify permissions granted by the user.

- **How can users be properly informed?**
    - Beyond the mere prior information, it is desirable for the user to continue to be informed during and following the processing.
    - As such, transparency measures on access to sensors, in particular via visual indicators on point access, when they are carried out by the system, but also when they are carried out by an application, specifying which one should be implemented.
    - The user should have access to a history of activation of sensors and queries made, filtered by use, system process or application.
    - For the most intrusive permissions (access to microphone, camera, geolocation, files on the phone, contacts, calendar), it should be planned to repeat the request for permission a few weeks after the first authorisation, so that the user can revert to his initial choice at the time he first implemented the application. In addition, an indicator could be displayed, for example in the status bar, signaling when permission is used.

- **How to facilitate data portability?**
    - The OS provider should implement portability of personal data, using an open format. This portability should concern configurations and applications installed on the phone.
    - Dialogue and cooperation with providers of other OSs should therefore be promoted, so as to define a ' *structured, commonly used and machine-readable format*', as referred to in Articles 4-1 and 20 GDPR, which is the most relevant for a user wishing to transfer his data from one OS to another.

3. Protecting Minor Users

The processing of data of minor users by application publishers is subject to special obligations. The AOS can provide useful tools for their implementation.

- **How to participate in application compliance for minor users?**
    - Parental control tools should be implemented within the OS that include, via an API or other non-intrusive technological modalities, the possibility of notifying applications of the relevant age range of the person. The parental control tool must be able to be used directly on the terminal without providing additional information to a third party (OS provider or publisher of a parental control system), or requiring the creation of a user account on an online service.
    - Such a solution would help app developers define whether the user is a minor, in order to facilitate compliance with GDPR obligations and minimise the need for remote processing.
    - The minority of users should be taken into account in these tools, regarding their ability to respond to system permissions through effective parental control tools.
    - It should thus be allowed to register several profiles within biometric authentication vectors, making it possible to distinguish whether it is the minor or his legal representative, so that it is possible for developers to configure an application where the minor's permission is sufficient for certain actions, and where permission of the legal representative would be necessary for other actions.

8.4. Provide a secure platform

The OS is the fundamental element in terms of terminal security. As such, OS providers should, as a good practice, ensure that they make available state-of-the-art elements to provide this guarantee to individuals.

1. Ensure the safety and partitioning of terminals

Security on mobile devices is mainly based on partitioning measures that ensure insulation of different applications.

- **How can application partitioning be implemented?**
  - The OS should ensure, via partitioning, the strict separation of applications between themselves and with the operating system, particularly in terms of memory access, but above all, in this context, of permissions.
  - If the terminal is used both in private and professional life, a partitioning of personal and business uses within the same terminal by means of technical and interface design measures should be put in place. For example, the following could be permitted:
    - the use of separate user profiles within the OS, communicating the existence of this functionality and encouraging its use;
    - the possibility of having several simultaneous and partitioned instances of the same application in order to allow simultaneous use according to the contexts.
  - The only partitioning per application is not always sufficient. Indeed, in order to ensure the granularity of permissions and the control of possible SDKs by publishers, it is also important to ensure a partitioning between the applications and the third-party codes they can invoke, in particular in terms of obtaining permissions. In practice, giving an application permission to access a resource should not automatically extend that permission to all SDKs embedded in that application.
- **What technical measures should be implemented?**
  - A secure storage space dedicated to local secret storage (enclave, otherwise known as “secureElement”) should be made available, when the terminal on which the OS will be run has the necessary hardware.
  - Encryption of network connections should be imposed. Otherwise, any unencrypted connection should be reported. The use of the TLS protocol should be forced as soon as possible, or its absence indicated to users.
  - State-of-the-art encryption features should be made available to applications.
  - Tools for local sharing between applications should be made available.
  - Backups should be encrypted by default, whether local or placed on third-party servers. Encryption keys should be kept on the terminal.
  - The OS provider should indicate best practices, accompanied by examples allowing developers to identify their users’ threat models and to put in place, where appropriate, additional security measures.

2. Provide effective audit tools

It is desirable that OS providers allow their users and professionals to audit the operation of the terminals to which they have access.

- **What tools should be made available?**
  - Adequate tools should be put in place, whether contained within the OS itself or offered in a development environment, allowing for a fine analysis of network traffic, running processes, and all communications, including those made to and from the servers of the OS provider.

- Official audit methodologies should be documented, e.g. for developers regarding their own applications but also of the treatments actually implemented by SDKs that they may be required to integrate for functionality or monetisation issues.
- Users should be able to generate simplified privacy reports, so that they can understand the impacts that certain applications may have.

3. Maintaining security over time

To ensure the security of terminals over time, the OS provider should put in place processes to ensure the maintenance of the user fleet.

- **How can terminal security be maintained over time?**
  - The OS provider should offer users support for versions of the OS as long as possible in time, in particular where an update from one version to another is incompatible, in terms of hardware restriction, on a significant part of the current terminal stock.
  - It should systematically offer security updates to the OS at least up to 5 years after the purchase of the terminal. The fact that certain functional elements are no longer compatible with the terminal should be insufficient to justify the cessation of security updates.
  - When this period has expired, the OS provider should clearly indicate to the person the risks associated with the failure to update. If they exist, the person should be directed to alternative OSs that support their terminal.

8.5. Checklist

Category	Sub-Category	Identifier	Description
Ensure compliance of the processing of personal data implemented	Identify and analyse the compliance of the processing of personal data implemented	1.1.1	An analysis of the responsibilities is carried out, covering the base of the AOS, the functional bricks added to it as well as the treatments that may be implemented by applications and used by people.
	Apply data protection principles by design and by default	1.2.1	No processing carried out on behalf of the OS provider shall be carried out prior to the receipt of a valid consent, including at the time of its first launch.
		1.2.2	Creating an account is not necessary to use the OS and pre-installed applications.
		1.2.3	The use of third-party notification servers is possible. Their use is optimised, especially in terms of execution in the background and impact on the battery.
		1.2.4	Tools to encrypt the content of notifications are offered, regardless of the notification server responsible for their transmission. The provision of these tools is accompanied by clear documentation.
		1.2.5	A bug lift and unannounced termination management system consistent with the

			principle of minimisation is proposed, including consent for the bug report to be raised.
		1.2.6	If a remote backup system of OS settings and content is offered, it is not enabled by default. It is the subject of a collection of consent and the corresponding data is transmitted and stored in an encrypted way,usinga key to which the provider of the OS itself does not have access.
		1.2.7	The availability of geolocation data may be limited only to the use of the GPS sensor, without mobilising further processing.
Ensuring that partners are properly informed	Provide comprehensive and clear documentation to support partner compliance	2.1.1	Documentation for third-party developers as well as documentation for OS end-users are up-to-date, easily understandable and comprehensive.
		2.1.2	Legal elements are present in this documentation, in order to promote the analysis and impacts of third-party developers and end users.
		2.1.3	The various documents are accessible in the languages of the target audiences.
		2.1.4	The documentation indicates how to implement consent requests within the AOS.
	Inform third parties of OS-specific processing	2.2.1	Partners (third party developers and publishers, application stores, builders, etc.) are able to know, understand and document, in accordance with the principleof *accountability* , the treatments involved or induced by the use of the AOS.
	Encourage the use of the most protective features	2.3.1	The APIs offered by the OS allow publishers and developers to meet their legal obligations.
		2.3.2	Updates to these APIs improve the previous point and specific documentation is offered to developers and publishers to accompany them in the use of these new APIs or new versions of APIs.
		2.3.3	Statistics and collections of developer feedback are put in place, in order to identify the most used features and, conversely, to communicate about privacy-friendly features that are ignored.

		2.3.4	Outdated API features and uses are documented and end-of-support dates are highlighted. Permissive features in terms of privacy are removed and developers are accompanied in updating their applications from features that have become obsolete to their replacements.
Provide tools to enable the rights and consent of users to be respected	Design permission systems that respect the principle of data protection by design	3.1.1	Access to physical sensors, network access equipment and terminal storage spaces can only be made after permission has been validated by the end user.
		3.1.2	Permissions allowing different levels of accuracy leave the end user, and not only the developer of an application, the choice of this level.
		3.1.3	Access permissions to the data present on the terminals make it possible to define and compartmentalise the storage spaces made accessible by these permissions.
		3.1.4	Permissions may be restricted by the user, over a time period and a number of defined occurrences.
		3.1.5	The execution of applications is designed so that they can be technically functional regardless of obtaining permissions.
		3.1.6	The technical documentation for developers refers to and encourages good practices so that their applications work with the strict minimum of permission granted and are accompanied by concrete examples of alternative methods they may consider (e.g.: collection of a postal code in a form rather than implementing a geolocation, documenting the implementation of this form).
		3.1.7	Users have the possibility to respond to a permission by a refusal of principle without it being a technical refusal. For example: following a refusal in principle, refer to the application of an empty contact book, an empty or partially empty photo library (storage *scope*), random geolocation, etc.
		3.1.8	Users have access to a detailed dashboard allowing them to view the permissions assigned and those that have been used, providing alerts for abnormal use of permissions.
		3.1.9	The permissions of an application are all

			revoked when an application has not been used for some time. The user is notified of this revocation.
	Assist in the proper respect of consent and users' rights	3.2.1	Permissions make it possible, in their format and contextualisation, to carry valid consent within the meaning of the GDPR and the ePrivacy Directive. In practice, they allow in particular to present the purpose of the processing, to list third parties and to specify the modalities of their revocation.
		3.2.2	Information is provided, regardless of that added by the app editor, to briefly explain the technical capabilities of permission, so that users can assess the benefits and risks of granting permission to a given application.
		3.2.3	Permission screens allow third-party developers to display to the user if permission is required for the operation of the application and the continued processing, or simply desired by the developer.
		3.2.4	Permissions can be easily revoked. Access to the menus allowing this revocation is intuitive.
		3.2.5	The current access to physical sensors, network access equipment and terminal storage spaces is the subject of a visual or audible signal within the OS interface presented to the end user (color pastilla, ringtone, vibration, etc.), allowing the user to determine which application is accessing which sensor.
		3.2.6	The user has a history of access to the aforementioned sensors, timestamp and per application.
		3.2.7	The OS offers data portability, within the meaning of the GDPR, allowing the user to migrate his data and configurations to another OS or to the same OS on another device, without the need for a creation or connection to an account.
	Protecting Minor Users	3.3.1	Parental control tools are made available to end-users.
		3.3.2	Age reporting tools are made available to developers, so that the use of their applications can be restricted or blocked depending on the age settings known to the OS.
Provide a secure platform	Ensure the safety and partitioning of terminals	4.1.1	A compartmentalisation(*sandboxing*)is implemented, allowing to limit and control interactions, access to memory and the use of permissions, between the

			OS and the applications.
		4.1.2	A compartmentalisation, both technical and interface, is implemented in the OS, in order to distinguish personal and professional uses on the same physical terminal.
		4.1.3	The implemented compartmentalisation makes it possible to restrict access to memory as well as the use of permissions to part of the application and not to its entirety. Specifically, it is a question of allowing a refusal of permission to one or more SDKs of an application, while allowing permission to be accepted to other SDKs or to the specific treatments of the application.
		4.1.4	Where the terminal hardware allows, local secret storage uses the dedicated hardware by default (enclave or '*secureElement*').
		4.1.5	A technical and interface constraint is applied to the implementation of network connections (e.g.: reporting of unencrypted connections, obsolete certificate, TLS forcing, etc.).
		4.1.6	Inter-application local sharing systems are made available bythe OS.
		4.1.7	A backup system of the OS, its configuration and its content is available to developers and end users.
		4.1.8	This backup system works locally by default. No remote backup is possible by default.
		4.1.9	This backup system, if it offers a remote backup, keeps the encryption key exclusively under thecontrol of the user.
		4.1.10	Good security design and development practices are shared with third-party developers.
	Provide effective audit tools	4.2.1	Audit tools and methodologies are available to developers and end users (fine analysis of network traffic, ongoing processes, etc.).
		4.2.2	Documentation of these audit tools and methodologies shall be made available in order to facilitate the work of those involved in using them and to ensure their full understanding of the results observed.
	Maintaining security over time	4.3.1	Support for each version of the OS is provided for as long as possible.
		4.3.2	Security updates are offered for as long

			as possible, at *least* 5 years, regardless of functional updates.
		4.3.3	When support for a version of the OS ends, clear information is provided to developers and end users.
		4.3.4	Each new version of an OS ensures the highest level of backward compatibility possible, so that mobile applications can be functional on a wide range of versions of the same OS.

9. Application Store Provider Specific Recommendations

Package leaflet

Who are these recommendations addressed to?

- These recommendations are addressed to app **store providers (*app stores* or *blinds* in English)**.
- In the context of these recommendations, the app store provider is **defined as the legal entity that develops and maintains an app store, i.e. a mobile app that indexes, promotes and allows the download of other mobile applications.** It may be a commercial entity or not, itself potentially legally linked to another entity (manufacturer, publisher, OS provider).
- In practice, for example, the target audience for these recommendations is:
  - the *Data Protection Officer* (*DPO*) of the entity providing the application store;
  - legal and technical teams of OS providers, in particular manufacturers, which have to authorise or integrate third-party application stores;
- These recommendations can also be consulted by mobile app publishers and developers who want to make their apps accessible in different app stores.

What is the purpose of these recommendations?

- While some operating systems allow the installation of applications following a direct download, the majority of users install applications via the default app store on their equipment. Regardless of the operating system used, the app store provider will generally not be responsible for the processing implemented within the applications themselves.
- The application store provider generally implements a review process for the proposed applications, whether for initial publication or updating, which may lead to the publication or rejection of the application on the store, most often as part of a process that allows the publisher to modify its submission to result in publication. It is also common for the app store provider, following reports or changes in its criteria, to suspend previously published applications.
- However, the provider of the app store can have a strong impact on the processing of personal data implemented through the applications when people use their devices. Its **design choices, the clarity of the information it offers and its ability to control the applications it makes available, before and during its making available, may have a significant impact on the rights and freedoms of individuals in their mobile digital uses**.
- As such, it is desirable for the app store provider to provide clear information on the processing that could be implemented within distributed applications and to implement processes that help ensure compliance with the applicable laws of published applications. **These recommendations are intended to assist app store providers in this process.**

How to use these recommendations?

- These recommendations are organised into several sections, each corresponding to a step in the app store provider's activity. **Each party outlines privacy issues and brings together a series of recommendations and good practices to be implemented**.
- These recommendations apply without prejudice to the rules applicable on other legal grounds than the protection of personal data, including competition law.
- **A consolidated checklist of key recommendations** for app store providers is proposed at the end of this section. App store providers are invited to study this list and

to use it in particular during checks carried out prior to the publication of an application in the store, as well as when updating the store's user interfaces.

9.1. Analyse applications submitted by publishers

In the process of reviewing applications that publishers request to be published in the app store, the store provider has the opportunity to collect information and analyse the proposed app in order to promote respect for end-user rights. The following recommendations apply in particular to applications targeting users within the European Union.

1. Centralise and analyse compliance data

In accordance with the principle of *accountability*, application publishers have an obligation to implement a whole set of processes and analysis of the processing of personal data which they will carry out in the context of the operation of the application. Thus, the provider of the application store can request the transmission of the pre-existing documentation created by the publisher in order to encourage good practices in terms of protection of personal data and increase transparency for users.

- **What information can be obtained from each application editor?**
  - The application store provider is recommended to request at *least the* following information:
    - the categories of data collected and the purposes pursued for each of the processing operations,
    - third parties who have or may have access to the data, which may include the list of SDK providers used,
    - the exhaustive list of system permissions requested by the application, including their mandatory or optional nature, and the purposes for which they are requested, as presented to the user when using the application,
    - the country in which the data will be stored and processed,
    - an update history, including updates notes.
  - It is recommended to request the provision of a contact point for users on privacy issues and the privacy policy;
  - It is recommended to allow applications to indicate whether they are aimed solely, mostly or potentially, at a minor audience.

2. Encourage better practices in terms of protection of personal data and privacy when publishing and updating applications

Due to their expertise, and often their extensive knowledge of operating systems, mobile app store providers appear to be prime players in encouraging the implementation of best practices when publishing and updating applications.

- **What good practices to encourage application compliance?**
  - In the process of reviewing applications, whether new or updates, it is recommended to encourage app publishers not to request bulk permissions during installation but rather to manage runtime permissions, enabling only those that will be required for the functionality used by end users only.
  - Similarly, it is recommended to invite app publishers not to use OS APIs that would be too broad or outdated, especially if the latest versions better comply with data protection principles by design and by default.

- **How to improve the update notes?**
  - Publishers should be asked to publish informative update notes for users. Update notes are a simple and accessible way for users to know in advance the consequences of updating their application.
  - This information is all the more important as the operating system implements software restrictions that prevent a version of an application from being downgraded. The user should thus have the choice, with full knowledge of the facts, whether or not to update his or her application, in particular if it is

functional, would not benefit from any particular security patch or be added additional processing of personal data.

3. Analyse applications to detect security flaws

Similarly, app store providers have the ability to provide app publishers with analytics tools to detect potential security vulnerabilities as soon as possible.

- **How to implement static analyses?**
  - Static analyses should be implemented before each release of an application, whether that publication corresponds to an initial publication or an update. Such analyses should be both automatic, manual and specific, in particular for applications exceeding a number of downloads or with features justifying further security and privacy analyses.
- **How can further analyses be carried out?**
  - For the most sensitive applications, dynamic analysis of applications should be implemented, both automatic and manual, in order to detect abnormal behaviors in use and escaping static analysis.
  - For example, it may be studied:
    - dynamic loading of ex- *post* software libraries;
    - execution in substantive tasks, which may, in particular, affect the battery life;
    - the use of behaviour specific to malicious applications, documented in particular in the scientific literature, specialised press and publications of CVE (*Common Vulnerabilities and Exposures*).

9.2. Implement transparent application review processes that incorporate the verification of basic data protection rules

It is important throughout the application publishing process that app store providers act with the utmost transparency and facilitate publishers' efforts.

1. Integrate the verification of basic data protection rules into application review processes

In order to support in their compliance with the GDPR publishers wishing to send an application to the European market, it would be useful for the application review processes to incorporate certain checks that can be carried out by the application store.

- **What data protection criteria should be included in the application review process?**
  - The publisher could be asked if the applications are aimed at the European market and verify who is informed of the applicable data protection rules. In case of a negative answer, the application should be prohibited on the versions of the store located within the European Union.
  - For publisher applications installed outside the European Union but aimed at the European market, the publisher should be asked if the application processes personal data. In this case:
    - the provision of a contact point for EU users wishing to exercise their rights should be required,
    - the publisher should be asked to submit in the review process the key data protection information: purposes pursued, data processed, procedures for exercising rights, retention periods,
    - advice on compliance with European data protection rules should be provided to the publisher.

- It would be useful for app stores to refuse apps that are not able to provide the above items.
- In addition, the app store provider could usefully offer users a mechanism for reporting applications that do not comply with the above rules, which could lead to an exclusion from the store application.

2. Clearly express expectations and processes implemented

To the extent possible, it would be useful for all stakeholders for app store providers to ensure clarity of security and privacy requirements for candidate applications.

- **What good practices for the information of application publishers?**
  - The provision of complete documentation on the points of requirement considered;
  - For each of these requirements, the publication of concrete examples of problematic behaviour, and solutions to address them,
  - The provision of a precise description of the validation process, the verification steps and the timing associated with each step, including for the various remediation processes in the event of rejection,
  - In the event of an update of the applicable rules, proactive communication to publishers concerning them, allowing a reasonable period of time for them to be taken into account. If these updates are intended to cause the rejection of previously accepted solutions, examples of remediation techniques may also be published.

3. Facilitate the use of tools made available

Application store providers should also ensure that they provide adequate tools for managing the release and resolution process.

- **Do app publishers have the tools at their disposal to effectively publish their application?**
  - The internal organisations of entities that publish applications can be very diverse.
  - As such, a fine management of access to the publisher accounts of the application store should be allowed. Thus, when several users participate in the publication of the application, this would allow them to have separate access to repositories, version signatures, update notes, as well as information useful to the user.
- **Do application publishers have an identifiable communication channel at their disposal?**
  - A clear channel of communication between the entities publishing mobile apps on the app store and the app store provider should be established, in order to avoid blocking situations.
  - The use of the publication platform for the implementation of the discard resolution process and subsequent communications with the organisation requesting publication should be preferred.

4. Be transparent on grounds for rejection and remedies

The need for transparency is particularly expressed in the event of refusal to publish. As a good practice, it is therefore important to implement mechanisms to ensure a good understanding of the decisions taken in this context.

- **Are the reasons for refusal and suspension sufficiently understandable?**
  - Transparent communication with mobile app publishers when applying the publication validity criteria should be ensured. The reasons for the rejection and

the appeal process that can be mobilised by the publisher should be indicated in a clear and precise manner.
- In particular, the reasons for the refusal and the proposed remediation methods should be specified in the documentation.
- If a security breach is detected, and in particular if this can lead to the deactivation of the application or communication to end users, the publisher should be informed in a reinforced manner.
- Communication with app publishers in their language is desirable.

9.3. Inform users and provide them with tools for reporting and exercising rights

For most mobile device users, app stores are the entry point of their uses. It is therefore desirable that access to these applications should provide them with a sufficient level of information, enabling them to exercise their rights more easily.

1. Standardise and make available compliance data

An app store most often has a search interface, giving a summary description of each application. Each application itself then has its own page, within which an important level of detail can be presented, to help inform the choice of potential users to download, or not, an application.

- **As a good practice, what information is displayed in the pages of each application?**
  - All the information referred to in section 9.1 (*"What information to obtain from each application editor?"*) should be made available to the user.
  - This information should be accessible prior to the purchase or installation of the application.
  - In the context of mobile interfaces, it can be complex to make all this information understandable. In order to make it easier to read, the use of graphic representations, e.g. the use of icons and tables, choosing them in such a way as to highlight the elements with the greatest impact in terms of privacy protection, should be preferred. The information made available could include information on how the application is financed, in particular where it is based directly on the re-use of the user's personal data for other purposes. Where appropriate, the information should be presented in a neutral and contextualised manner.
- **What information can be displayed in the search interface?**
  - Filters containing privacy criteria could be made available directly in the search interface. These could relate to the use of certain permissions, the collection of certain data or even a 'score' relating to privacy criteria.
  - If the creation of such a score is envisaged, it should be based on a methodology previously defined and transparent, preferably by an actor outside the app store provider and ideally agreed between the different ecosystem and civil society actors. The process of calculating this score is likely to be the subject of certification, in particular to ensure that it meets its objectives in terms of transparency. Source data should also be made available to calculate this score in an open and easily actionable format, so that alternative methodologies can be proposed.
  - The parameters that can be taken into account in drawing up this score may include:
    - the types of data collected (depending on their sensitivity), their volume and the purposes pursued,
    - the number and type of permissions requested by the application from the moment of installation, as well as those that may be requested in the short term of use of the application,
    - the number and type of SDK included in the application and the data they collect according to the purposes,
    - the security measures implemented,
    - the possibility to have access to the source code of the application.

2. Make available clear reporting arrangements

The interface of the application store is a privileged channel to allow users' feedback to be taken into account

- **How to make use of user feedback and reporting?**
  - Users should be allowed to report applications that do not fulfil their obligations directly from the app store, in particular in terms of exercise of rights, deceptive design (" *dark patterns*") of breaches of consent, execution of SDK functionalities without prior consent, presence of unframed transfers, etc.
  - These reports could be used to guide controls on published applications and also impact the score on private life criteria.

3. Prevent in case of vulnerability detection or need for updating

The app store is, technically, the most capable player to massively protect users from security risks. As a good practice, it can therefore participate in the protection of users.

- **What to do if active vulnerabilities are detected?**
  - The application store provider should establish a protocol to be adopted in case of revelations of vulnerabilities in an application that could affect a significant part of the store's users, in particular where the detection of the presence of that vulnerability can be analysed (including statically) on a large scale in terms of the number of applications involved.
  - Once vulnerable applications are detected, several measures can be applied, sometimes simultaneously. For example, consideration may be given to:
    - suspend automatic updates of all or part of the user fleet;
    - temporarily remove all vulnerable applications, making it impossible to download them and protect potential and future users, until they have been updated and this update does not pass the security test established when detecting vulnerable applications.
  - The app store provider should also analyse whether user information is needed. If the vulnerability poses high risks to data subjects, it may be considered, for example, to display a system notification to users, indicating that one or more of their applications are vulnerable.

9.4. Checklist

Category	Sub-Category	Identifier	Description
Analyse applications submitted by publishers	Centralise and analyse compliance data	1.1.1	For each publication submission (new application or new version), the information required by the publisher shall include at *least*: • the data collected and the purposes pursued for each of the processing operations; • third parties who have or may have access to the data, which may include a list of SDKs used; • an exhaustive list of the system permissions requested by the application, including their mandatory or optional nature, and the purposes for which they are requested, as presented to the user when using the application; • the country in which the data is stored and processed; • an update history, including updates notes.

		1.1.2	A privacy policy and point of contact are defined and accessible to end users, for each application editor having at least one app published in the store.
		1.1.3	When an application is intended only, mostly or potentially for a minor audience, this information is indicated on the store page relating to that application.
	Encourage better practices when publishing and updating applications	1.2.1	Before submitting an application version application for validation, publishers are advised not to request block permissions during installation and are encouraged to have permission management at runtime, activating only those that will be required according to the features used by end users.
		1.2.2	Publishers are advised not to use OS APIs that would grant too broad permissions or would be outdated, especially when the version of the OS detected by the store allows better compliance with data protection principles by design and by default.
		1.2.3	Publishers are asked to publish informative update notes for users, in order to allow end users to define themselves whether or not they want to install a new version of the application, especially in the event that the update is only functional, without providing security fixes.
	Analyse applications to detect security flaws	1.3.1	Static analyses are performed on each new application or application version, prior to publication in the store.
		1.3.2	Dynamic analyses are carried out on new versions of applications exceeding a number of downloads, prior to any publication in the store, in order to detect points of non-compliance that would result from their behavior over time and use.
Implement transparent application review processes that incorporate the verification of basic data protection rules	Integrate the verification of basic data protection rules into application review processes	2.1.1	Up-to-date and comprehensive documentation of pre-publication requirements is made available to publishers, to which are attached concrete examples of elements and behaviours blocking or problematic to publication in the store.
		2.1.2	Publishers are asked if their application is aimed at the European market. If this is not the case, the application is not available on stores located within the European Union.
		2.1.3	If the application, conversely, targets the

			European market, several elements should be requested from its publisher, including the provision of a contact point for the exercise of the rights of individuals as well as the implementation of the principles of the GDPR, such as the purposes pursued, the data processed, the retention periods, etc. If the application is aimed at the European market but is unable to provide these elements, it shall not be published on the store.
	Clearly express expectations and processes implemented	2.2.1	App publishers are properly informed, in particular about the compliance elements that are incumbent on them according to the store's criteria. The update of these elements, over time, is communicated to them.
	Facilitate the use of tools made available	2.3.1	Fine management of access to app store publisher accounts is proposed, so that multiple users can have separate use of repositories, version signatures, update notes.
		2.3.2	A clear channel of communication between mobile app publishing entities and the app store is displayed, favoring a channel integrated into the app store itself.
	Be transparent on grounds for rejection and remedies	2.4.1	The refusals to publish and the patches to be applied to overcome this refusal are clearly indicated to the publishers and are based on the dedicated documentation elements.
		2.4.2	Specific care shall be taken to ensure the completeness and clarity of the explanations provided to the publisher whose version of the application is refused where such refusal is, in whole or in part, due to a security problem involving a risk for the data subjects' data.
		2.4.3	Exchanges and explanations given to publishers in the validation process take place in the language declared or desired within their profile
Inform users and provide them with tools for reporting and exercising rights	Standardise and make available compliance data	3.1.1	All information relating to privacy, transmitted by the publishers or known from the store, is accessible to the end user before purchase or download.
		3.1.2	All the information required or useful to the end user shall be displayed in a format adapted to the system in which it is to be consulted.
		3.1.3	Privacy filters are offered among the search options.

		3.1.4	Privacy information should be published in a comprehensive and synthetic manner. To do this, this information is first provided in a synthetic format, allowing for example the display of a privacy score, and secondly exhaustively, for example by clicking on a 'Learn more' link.
		3.1.5	A score for privacy settings is displayed on the apps available in the store. Preferably, this score is based on a methodology defined beforehand, in a transparent way so that it can be certified and defined by one or more actors outside the application store itself.
	Make available clear reporting arrangements	3.2.1	End-users have the ability to report applications that would not fulfill their obligations, directly from the store.
	Prevent in case of vulnerability detection or need for updating	3.3.1	A protocol is defined for the actions to be taken when detecting, via static or dynamic analysis, a vulnerability within a mobile application already published in the store.
		3.3.2	A specific display is offered to end users, integrated into the app page in the store, on a potential security risk. For example, it may be the detection of a software library that is considered vulnerable but would pose a risk only in the context of certain applications, without it being possible to define it *a priori*.

10. Glossary

Software development *kit or* SDK:

The software development kit refers to a set of tools used for the development of the application, depending on the operating system used. This practice, which is highly developed in the mobile ecosystem, is due in particular to the fact that SDKs most often facilitate or accelerate the development of software features, avoiding the developer from writing the entire code of the application. These SDKs are usually integrated by the addition of the code offered by them in the developed application, which will eventually allow to interface with the infrastructure of the SDK provider to implement the functionality. They cover many features, but the most common ones are *analytics*, selection and delivery of advertisements or e-commerce features.

Mobile application:

The concept of mobile application refers to application software distributed in the environment of multifunction mobile (or " *smartphones*") and tablets, i.e. individual and portable terminals, allowing access to the Internet network and, most often, to the telephone network, and which can allow the installation and execution of third-party applications within them. These applications are run in isolation (or in "sandbox" mode) by an operating system that limits the functionality they can access via a permission system.

Execution 'in sandbox' or ' *sandboxing*':

Sandboxing is a security mechanism implemented by *an* operating system to isolate an application executed from the core of the operating system but also from other applications running on the terminal. This isolation reduces the risk that could be associated with misuse of terminal features, but also attempts by an application to access data or disrupt the operation of a third-party application. In general, applications running in sandbox mode have fairly reduced default features, having the option to use only APIs provided by the OS, subject to user permission.

Application Programming Interface (API)

An API (*application programming interface* or "application programming interface") is a software interface that connects a software or service to another software or service in order to exchange data and functionality.

APIs provide many features, such as data portability, setting up advertising email campaigns, affiliate programs, integrating features from one site to another, or accessing open data warehouses. Their access can be free or paid.

In the context of mobile applications, APIs are also the means by which the operating system exposes a whole set of features to applications.

Operating *system* (OS)

The operating system is the software brick closest to computer hardware, allocating available resources (computing resources, memory, access to devices) to the different application elements that request it.

In the context of mobile applications, the OS is the software brick that defines and allows all possible interactions between the user and the terminal, but also between third-party mobile applications (i.e. those added a posteriori) and the terminal. In particular, it implements the " *sandboxing*" execution of the applications, as well as the permission system allowing access to the terminal's functionalities.

Access permission

Access permissions are devices implemented by mobile device OSs to allow users to choose which features are accessible to mobile applications. These mobile applications only have limited access to these features by default, for reasons of security and privacy. The OS therefore provides them with APIs allowing them to make queries in order to be allowed additional functionalities, provided that the user, via an interface provided by the OS, accepts it.

Audience measurement (' *analysis*')

The management of a website or mobile application may in many cases involve the use of services to collect traffic or performance statistics, usually grouped under the term audience measurement or 'analysis'. These tools can in practice be of a very diverse nature, ranging from very simple measures which can sometimes prove essential for the proper management of the service to tools offering complex analysis features, such as "A/B testing" or " *AB testing*" (presenting different versions of the site to different users), heat maps or heatmaps *(* presenting the aggregation of user navigations) or session replay (allowing to visualise the path of a single user). Some commercial tools (for analysing sources of traffic or targeted advertising) are sometimes misrepresented as audience measurement solutions.

Advertising ID

Advertising identifiers are numeric identifiers, often represented as strings, generated and associated with a terminal by the OS, and which may, under certain conditions dependent on the OS in question, be made available to applications that request it. Those identifiers are specifically designed to enable the identification of a single user by different applications, which is made impossible by the *sandboxing* of the applications outside it. This identification allows in particular advertising targeting. For example, if a user is logged into a social network from his or her phone and third-party applications embed the targeting module of that social network, access to the advertising identifier will allow the person's profile data to be used to target advertising in the context of those third-party applications.