Recommendation

on mobile applications

Published on 8 April 2025 (Deliberation *No 2025-024 of 27 March 2025 amending the Recommendation on mobile applications and repealing Deliberation No 2024-061 of 18 July 2024 adopting the Recommendation on mobile applications*)

Courtesy translation. Only the French version is legally binding.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table of contents

1. Introduction

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

For its users, the 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 to which mobile applications have access. However, the data processing implemented within applications can be or appear opaque. In particular, information on the existence of data collections and their objectives is often unclear. Users may find it difficult to understand the nature of the permissions requested, which makes it difficult to express their choices. Finally, smartphones include many sensors more or less known to users (camera, GPS, contact database, accelerometers, etc.) and which can allow applications to access data whose collection can be very intrusive.

Stakeholders involved in the provision of mobile applications must ensure compliance with their data protection obligations and users' rights. There are many such stakeholders: application developers (some of which can exchange data), operating system providers, application store providers, software development kits (SDKs) providers linked to social networks or technical functionalities, etc.

In practice, data exchanges often take place between these different entities, with sometimes poorly defined sharing of responsibility. In particular, the use of SDKs processing personal data in a non-compliant manner and the non-compliant use of mobile identifiers have already been the subject of formal notices or penalties on the part of the CNIL.[1]

While data protection principles and obligations are now well known to website operators and are the subject of recommendations by the CNIL,[2]their implementation in the context of mobile applications needs to be clarified.

This Recommendation aims to clarify these rules so that stakeholders in the mobile ecosystem have a good understanding of their obligations and proposes concrete recommendations to comply with them as well as best practices.

These recommendations are without prejudice to the applicable rules on other legal grounds than the protection of personal data, in particular competition law and Regulation 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (the *Digital Markets Act* or DMA).

[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 (this decision is the subject of an appeal before the Council of State on the date of adoption of this recommendation), Dec. n° SAN-2022-026, 29 Dec. 2022.

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

2. Scope of the recommendation

2.1. Who is this recommendation addressed to?

This recommendation aims to recall and clarify the law applicable to the processing of personal data of users of mobile applications. It should guide mobile application environment professionals in their compliance with data protection regulations.

It is aimed at professionals working in the mobile applications sector, namely:

- application publishers;
- application developers;
- SDK providers;
- operating system providers;
- application store providers.

This recommendation is particularly addressed to professionals with an impact in terms of personal data protection, for example data protection officers. It is also used for all personal data protection advice.

It must help each professional to determine his legal qualification within the meaning of the GDPR (joint controller or processor), in order to better understand his obligations.

The obligations, recommendations and best practices arising from these qualifications are detailed in the sections dedicated to each stakeholder. However, each stakeholder is invited to refer not only to the recommendations that concern him or her but also to those addressed to his or her partners in order to better understand the obligations of each stakeholder.

2.2. What is meant by "mobile application"?

The concept of mobile application refers to application software distributed in the environment of smartphone and tablets, that is to say, individual and portable terminals, allowing access to the Internet and, most often, to the telephone network, and which may allow the installation and execution of third-party applications within them. This includes all typologies of applications, whether used in a private or professional context.

- These applications are most often distributed via broadcast platforms integrated into the terminal by the manufacturers and are run on it in isolation from each other (sandbox model). Applications can access a number of system features and data via application programming interfaces (APIs) made available for this purpose by the operating system provider (OS).

- This Recommendation covers all types of application, 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, then transformed into applications using specific tools (such as React-Native or Flutter), in order to maintain a uniform code base over time across all versions of the application;

    - “Progressive Web App” (“PWA”), i.e. dynamic web pages that are presented to the user in the form of applications.

How does this Recommendation apply to software environments similar to those of smartphones?

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 that allow the distribution of applications on a mobile operating system adapted to a specific use, for example:

- connected watches, smart speakers*;*
- connected car dashboards;
- connected personal medical devices;
- sensors and objects connected to the Internet ('Internet *of Things'* or 'IoT') in general;
- individual IT (Windows, MacOS, Linux, etc.);
- certain dedicated environments (e.g.: video games on Steam).

2.3. Who are the stakeholders in the mobile applications sector?[3]

Multiple stakeholders are involved in the mobile application ecosystem and process personal data in different ways. These are mainly the operating system provider, the application store provider, the application publisher, the developer and the SDK providers. Most often, these stakeholders are interdependent.

Operating system providers

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, in which environment the application will subsequently 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 stakeholders may be involved in the construction of an OS as it will be used by the end user.

Thus, a third-party OS provider may choose to use the code base of another OS 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 functionality 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 it has not developed itself and that it has chosen to integrate into its own system (e.g.: office suites, mobile phone operator applications).

This is for example the case for smartphone manufacturers that use an *open source* technical base and integrate third-party software components[4] as well as their own applications. This is also the case for mobile phone operators offering smartphones including a bundle of pre-installed services.

The recommendations apply to all stakeholders involved in the provision of this functional building block.

What processing of personal data is involved?

The OS generates identifiers specific to each terminal or user account specific to the OS, which, alone or in combination with other data, enable 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 may be passed on to third parties, including application publishers.

[3] This section aims to present the stakeholders operating in the mobile applications sector. Refer to Part 4 of these recommendations for the roles of each stakeholder in the use of the application.

[4] In 2023, some manufacturers (e.g. Samsung, Oppo, Xiaomi) thus use the AOSP technical base made available by Google (Android Open Source Project: *codebase of the open source*Android operating system) 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) as well as their own applications.

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, terminal location, accelerometers, etc.) as well as the data stored on the latter (contact book, photo gallery, list of installed applications, etc.).

Application stores

What is the role of the application store provider?

The application store provider shall make available the online distribution platform for applications.

This platform is accessible on the user's device 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 connection between the application store and the operating system?

The application store provider is frequently, but not systematically, the operating system provider. However, a specific application store may also be offered by the terminal manufacturer (Samsung, Huawei, etc.). Finally, concerning in particular the Android operating system, many application stores are also available, offered by third-party non-builders, and can most often be installed as standard apps (F-Droid, Aurora Store, etc.). The application store can set the rules applicable to apps and condition their publication in the store, for example in terms of security measures or user information.

What processing of personal data is involved?

The establishment of the rules relating to the application verification and validation procedure does not in itself imply the processing of personal data.

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

Application publishers

What is the role of the publisher?

The publisher makes the application available to users (most often through an application store) to offer its products or services. It also defines its economic model.

What processing of personal data is involved?

The publisher processes, in the majority of cases, personal data when using its application: technical connection data, data provided by the user or already present on his terminal, data inferred from his navigation, etc. It can thus be data necessary for the provision of a good or service through this application (contact, payment, location data, etc.), as well as data related to the operation of the application itself (technical data to ensure the proper functioning of the application, verification of the compatibility of the OS version, etc.). The publisher may also transmit the data collected to third parties, in particular for the purposes of monetising its audience, via various means specific to the mobile ecosystem (establishment of tracking devices specific to the mobile environment, provision of the user's mobile identifier, etc.).

Application developers

Who is the developer of the application?

The publisher of the application may 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, publisher and developer are two separate contractually linked entities.

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

What processing of personal data is involved?

By participating in the development, the developer of the application configures future processing of personal data. By participating in its maintenance (pre-production tests, data analysis, error reports, etc.), the developer can 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) refer to a set of tools used for development, e.g. mobile applications, 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 make it possible to facilitate or speed up the development of software features, by making it possible to avoid the developer writing the entire code of the application.

What is an SDK in practice?

This is a third-party software brick installed in the application. While the SDK may allow operations to be carried out locally on the terminal, in many cases the 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 be used to implement certain functionalities in the application (e.g.: payment, sharing on social networks, etc.).

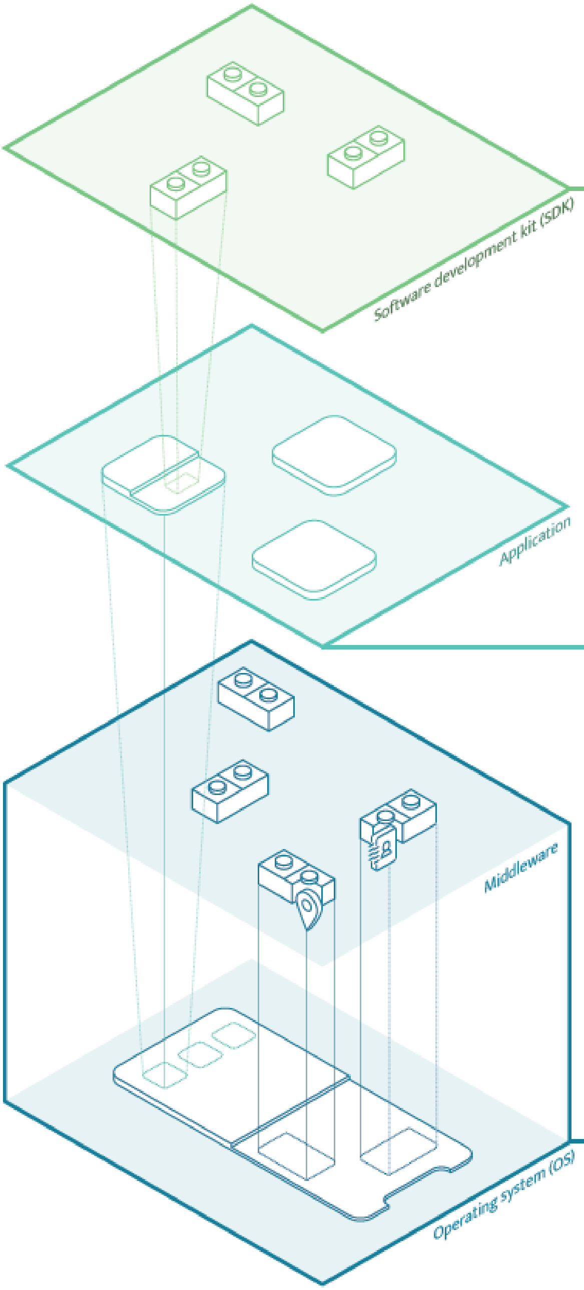
Other SDKs make it possible to make requests for access to the OS, such as the unique advertising identifier associated with the terminal or its location, and thus to track the user of the application for different purposes, for example for advertising purposes.

What processing of personal data is 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 bricks, depending on the characteristics and purposes of each SDK, and sometimes assume responsibility under the GDPR.

This may include, for example:

- processing consisting of offering certain functionalities through the application, for example image analysis or processing (reading QR code, augmented reality, etc.);
- processing operations consisting in tracking users for the purposes of data analysis (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 track its users and establish profiles for the benefit of third-party advertisers or advertisers, to monetise its audience.



SDK providers

The **SDK provider** is the entity that **makes a software development kit available.**

In practical terms, a SDK is a set of software functions, or blocks of code, designed to be integrated into predefined systems.

That distinguishes it from the mobile application developer: **a SDK cannot run on its own, it needs to be integrated into an application in order to function.** For this reason, a SDK supplier will have many partners: developers and publishers, including mobile application publishers.

Application publishers and developers

A mobile application developer is the individual or legal entity that actually **writes the code** for a mobile application.

The mobile application **publisher** is the entity that **publishes a mobile application in a store** or on its own platform.

In many cases, the publisher does not have its own development team. In this case, the publisher calls on the services of developers, who will then produce the application code on its behalf.

OS providers

In practice, several stakeholders may be involved in the development of an operating system.

For example, a third-party OS supplier may choose to use the code base of another OS and then integrate software overlays into its own OS.

Middleware is the third-party software components included in the final version of an operating system, as it will be offered to users. In practice, these are usually mobile applications that the manufacturer of the mobile device has not developed itself and that it has chosen to add to its own system. As these applications are pre-installed, it is in principle impossible for the end user to uninstall them.

The **OS supplier**, on the other hand, is **responsible for the final version of the system**, as it will be used by people. In practice, this term most often refers to the **manufacturer of the mobile terminal**.

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

The recommendations apply to operations implemented through an application:

- reading and writing operations on the mobile terminal as defined by Article 82 of the French Data Protection Act, pursuant to Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications ('the ePrivacy Directive'), whether or not they relate to personal data.

- Transactions 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 into Article 82 of the French Data Protection Act, is applicable if a reading or writing operation is carried out on the user's terminal via an electronic communication network, namely 'any *action to gain **access, over an electronic communications network,** to information already stored in his electronic communications terminal equipment, or to **store** information in that equipment'* (Article 82 of the French Data Protection Act).

This is particularly the case, where they are transmitted over a network, of:

- The **use of identifiers specific to the mobile environment** (terminal unique identifier, MAC address, etc.)[5] or other tracking techniques such as ***fingerprinting***[6]**;**
- **access to certain information contained in the terminal** (photo gallery, contacts, etc.);
- **access to certain terminal sensors (camera,** microphone, location, etc.);

Focus: the role of mobile identifiers

- In the mobile application ecosystem, identifiers specific to that environment make it possible, alone or in combination with other information, to track each user in a unique way.
- They may be linked to the mobile terminal on which the operating system is installed (including the unique advertising identifier)[7], or to the account of the authenticated user within the operating system environment[8], or they may be associated with an installation of the application. In the first case, these identifiers allow advertising partners and publishers to uniquely identify the terminal in each application installed on the operating system in order to adapt editorial content and advertising personalisation according to the characteristics and behaviour of the user. In the second case, they

[5] See point 13 of the CNIL amending guidelines on *cookies* and other tracking devices. The use of mobile identifiers has given rise to sanctions both from application publishers (see Dec. No SAN-2022-026, 29 Dec. 2022) and from application stores (see Dec. No SAN-2022-025, 29 Dec. 2022, this decision is the subject of an appeal before the Council of State on the date of adoption of the recommendation).

[6] Tracking via an identifier calculated from the technical information of the terminal

[7] For example, in the Apple environment, this is the advertising identifier attached to each device ('Identifier for Advertisers' or 'IDFA') or the identifier common to the applications of the same publisher ('Identifier for Vendors' or 'IDFV'). 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 at 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 relating to an individual. Coupled with an authenticated environment, they also make it possible to link this data to an activity on other terminals of the user on which the user is also authenticated. This may allow advertising partners to value the data collected on a user in the context of one application by offering them targeted advertisements in other applications. It also increases the potential intrusion of this technology into the privacy of smartphone users.

[8] For example, the UDID in the iOS environment (Apple), for 'Unique Device IDentifier', which identifies an Apple device (iPhone, iPad, etc.).

allow the operating system provider to track users on its own behalf and purposes and cannot in general be used by third parties.

- These identifiers can thus be passed on to third parties (in particular application publishers, but also advertising partners).
- These identifiers may be unique (i.e. the same identifier is provided to each application having access to them, which facilitates cross-application tracking for third parties) or specific to each application publisher.

What are the consequences?

Internet users must be **informed** and give their **consent** prior to these storage or gaining of access to information stored in the terminal operations, unless these actions are strictly necessary in order to provide an information society service explicitly requested by the user or have the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network (see Article 82 of the Data Protection Act and CNIL, deliberations No 2020-091 and No 2020-092 of 17 September 2020[9]).

The data processing carried out on the basis of the data retrieved through those operations (also known as 'subsequent processing') must, moreover, be based on one of the legal bases provided for by the GDPR. [10]

3.2. Application of the GDPR

Material scope

The GDPR applies to all processing of personal data carried out by the application.

Territorial scope

The GDPR applies (Article 3):

- to the processing of personal data carried out in the context of the activities of stakeholders (controllers or processors) established in the territory of the European Union (EU), 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 with its only establishment in the territory of the European Union;
- to the processing of personal data of persons who are on the territory of the EU and carried out by actors (controller or processor) who are not established in the EU, where the processing activities are related to (i) the offer of goods or services to such persons in the EU or (ii) the monitoring of the behaviour, within the EU, of such persons. Thus, the GDPR will apply to processing carried out by an application intended for persons in the EU and which processes the data of those same persons, even if the processing is carried out by actors located outside the territory of the European Union.

3.3. Processing covered by the household exemption

Household exemption: What is it?

The GDPR does not apply to the processing of personal data falling under the domestic exemption, i.e. processing carried out by a natural person in the context of 'personal' activities (activities specific to the activity of a single individual and carried out in principle in a non-professional context) or household activities (activities common to a limited number of people, in a family or friendly context) (Article 2.2.c and recital 18 of the GDPR).

[9] 'Cookies and other tracking devices: the CNIL publishes amended guidelines and recommendation',cnil.fr
[10] 'Cookies and other tracking devices: the CNIL publishes amended guidelines and recommendation',cnil.fr

Household exemption in the texts

Article 2.2.c of the GDPR:

'[The GDPR] *does not apply to the processing of personal data … by a natural person in the course of a* ***purely personal or household activity.'***

Recital 18 of the GDPR:

"This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities."

What are the consequences?

Processing benefiting from the household exemption is not subject to the provisions of the GDPR.

The means of processing provided by third parties may also not be subject to the GDPR, under certain conditions (recital 18).

In which cases does the GDPR not apply to the means of processing provided by third parties in the context of processing covered by the household exemption?

The CNIL recommends analysing the following two cumulative criteria in order to determine whether the means of processing provided by a third party are not subject to the GDPR:

- the processing is initiated at the discretion of the person (here the user of the application), carried out under their control and solely on their behalf, i.e. decided and implemented by them;
- the processing is carried out in a compartmentalised environment, i.e. without the possible involvement of a third party in this data: the third party has provided the means of processing, but it can no longer act downstream on the data.

The CNIL considers that, in those circumstances, the actor merely provides software to the user's service. The GDPR is not applicable to the software provided.

In other cases, the third party that processes the data at the request of the person is likely to assume some form of processing responsibility for the application of the GDPR, either as a controller or as a processor.

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

Thus, the CNIL considered that the GDPR did not apply, under certain conditions, to the means of processing provided by application publishers in the following cases:

- Biometric authentication in smartphones: this is the case when the processing is carried out on the sole decision of the user, with only local and encrypted storage of their biometric data. Indeed, the processing is carried out at the discretion of the person, and the data remain entirely under tehir control;
- Health mobile application: this is the case where the application records and stores data only locally, without an external connection and for exclusively personal purposes, without the application offering functionalities 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 it. The processing is carried out at the discretion of the person, who only uses the application for personal use.

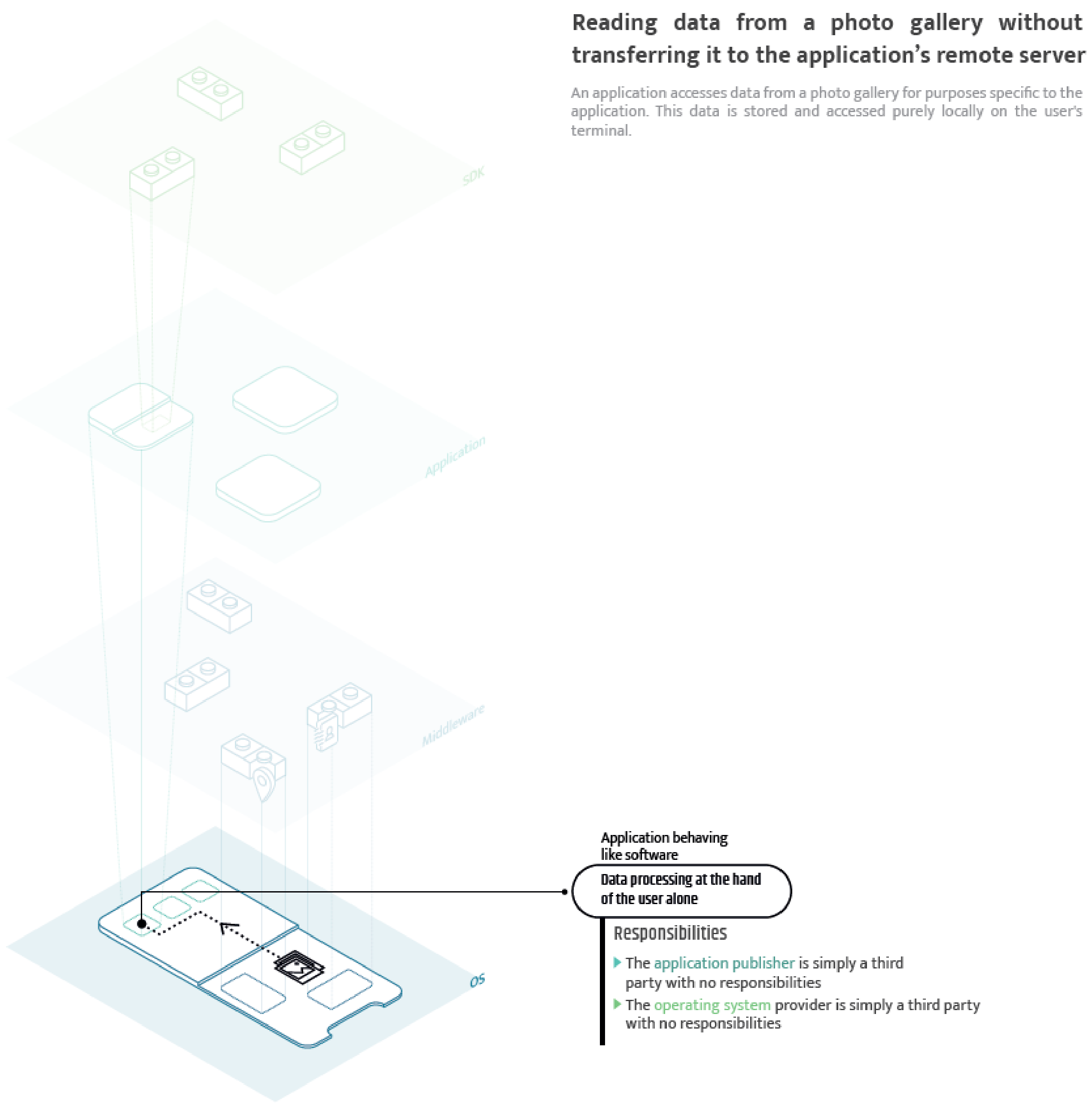
The same reasoning may apply to application publishers providing the means of processing in the following cases:

- Sharing data 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 and operating without exchanging data with a third party, apart from occasional updates (e.g.: keyboard with local scalable configuration

["learning"] without federation, functionalities involving only statically pre-recorded data in the application).

Example: reading data from a photo gallery without transferring it to the application’s remote server

An application accesses photographs for purposes specific to the application (e.g. to enable retouching of the photographs). These data are 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 interfere in any way with 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, in so far as they determine neither the purposes nor the means of the processing of the data.



Reading data from a photo gallery without transferring it to the application’s remote server

An application accesses data from a photo gallery for purposes specific to the application. This data is stored and accessed purely locally on the user’s terminal.

Application behaving like software

Data processing at the hand of the user alone

Responsibilities

- The application publisher is simply a third party with no responsibilities
- The operating system provider is simply a third party with no responsibilities

The CNIL considers it a good practice to offer mobile applications based on processing carried out entirely on the initiative and under the control of the person according to the conditions defined above: these applications and the resulting processing ensure data protection by design.

The CNIL encourages publishers and developers of this type of application to follow the following best practices:

- ensure the security of their applications, in particular by keeping the versions of their applications up to date and delisting applications that no longer need to be used due to software vulnerabilities;
- Design their applications in line with the GDPR's data minimisation and security principles to limit the risks users face in the event of a data breach.

What is the classification of the application publisher providing the means of household processing if the GDPR is applicable to it?

The GDPR applies to the means of processing provided by the publisher of the application, where the latter does not comply with the conditions specified above. In this case, the publisher may in particular be classified as a controller if it defines the purposes and means of the processing.

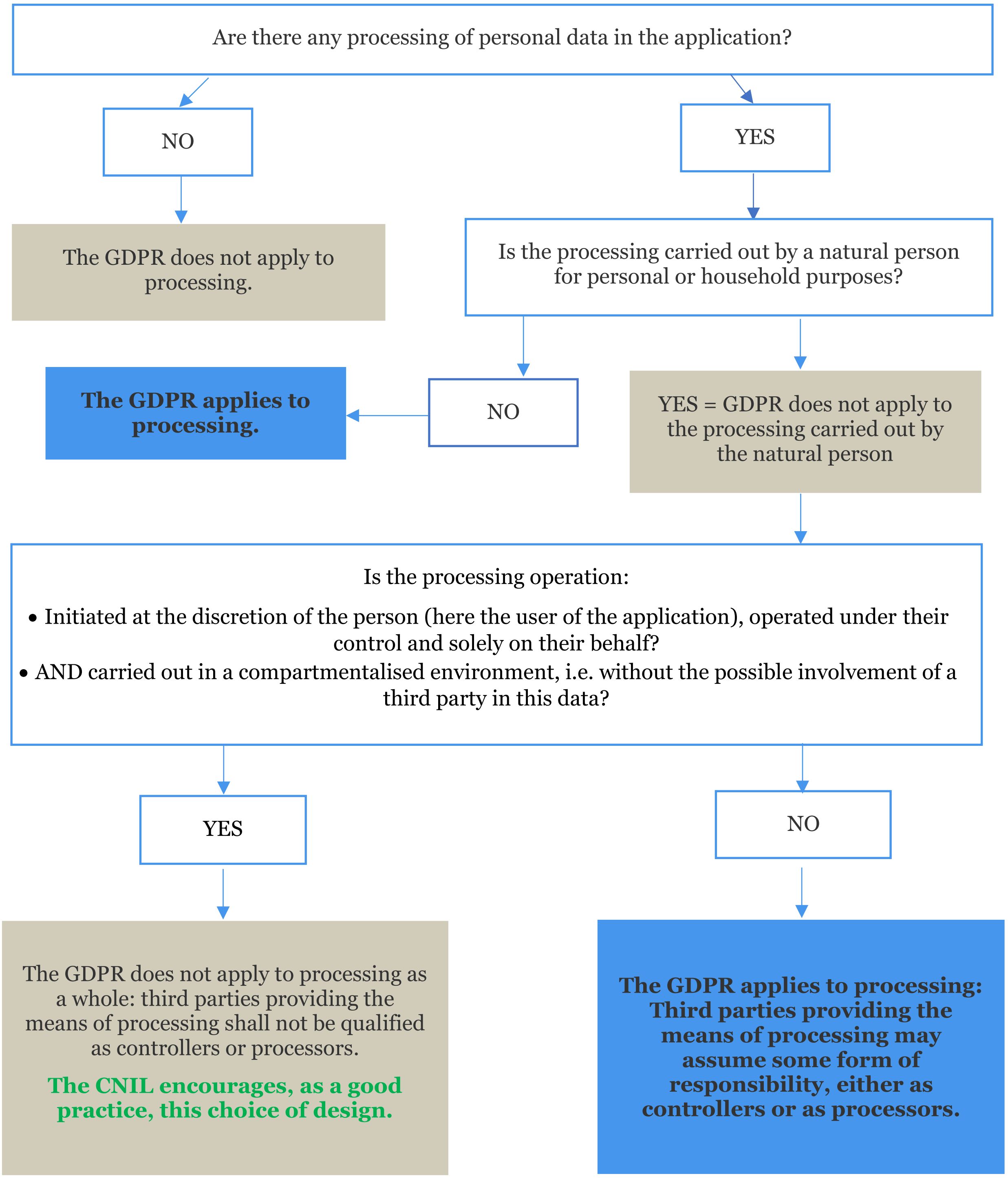
Example: creation of a shared family photo album within a photo gallery app

A family uses an app to create photo albums. Albums are shared among all family members using this app in order to share photos between different users.

In that case, the GDPR does not apply to the processing relating to the photo album because it is carried out by a natural person in the context of a purely household activity, for the purpose of sharing family photos with family members.

On the other hand, the publisher of the application may assume processing responsibility within the meaning of the GDPR if the album is stored on its servers or those of third parties. Its role within the meaning of the GDPR (controller or processor) is analysed in the light of the circumstances of the case and in particular the purposes pursued.

To keep in mind: questions to ask yourself as an SDK developer, publisher or provider to determine whether the GDPR applies to the processing implemented in the application


Are there any processing of personal data in the application?
NO
YES
The GDPR does not apply to processing.
Is the processing carried out by a natural person for personal or household purposes?
The GDPR applies to processing.
NO
YES = GDPR does not apply to the processing carried out by the natural person
Is the processing operation:
• Initiated at the discretion of the person (here the user of the application), operated under their control and solely on their behalf?
• AND carried out in a compartmentalised environment, i.e. without the possible involvement of a third party in this data?
YES
NO
The GDPR does not apply to processing as a whole: third parties providing the means of processing shall not be qualified as controllers or processors.
The CNIL encourages, as a good practice, this choice of design.
The GDPR applies to processing: Third parties providing the means of processing may assume some form of responsibility, either as controllers or as processors.

References

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

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

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

The stakeholders involved in the mobile application environment do not all 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;[11]
- Joint controller;
- Processor.[12]

Controller

Determines the purposes and means of the processing

For example*, I am responsible for the processing as data controller if:

I decide on the creation of the processing

I define the "why" and "how" of the processing

I have decision-making power

...

Joint controllers

Determine jointly the purposes and means of the same processing

For example*, I am a joint controller if:

I decide jointly with another the purposes and means of the processing

These decisions are convergent, complementary and necessary

Processing is not possible without the involvement of the identified joint controllers

...

Processor

Processes personal data on behalf of, on instructions from and under the authority of the controller.

For example*, I am a processor if:

I provide the service at the request of the controller

The controller specifically mentions the processing of personal data in the contractual elements

The processing of this data is a key part of the service I provide

The controller controls how I provide the service

...

[11] Natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing (article 4.7 GDPR).
[12] Natural or legal person, public authority, department or other body which processes personal data on behalf of the controller (article 4.8 GDPR).

[*]These are examples of non-exhaustive indicators supporting the qualification.

Other stakeholders may be contractually involved in the design, development, distribution and operation of a mobile application, without any of these three qualifications.

In accordance with the principle of *accountability* laid down by the GDPR, each stakeholder must determine its qualification in the light of its actual role for each processing of personal data, following the criteria defined by the EDPB.[13] They must be able to explain the classification adopted, specifying the reasons which led to the choice of that classification, and in particular: who decided to create the processing ? who defined its purpose ? who determines the personal data collected, their retention periods, the security measures put in place?

Stakeholders must demonstrate that such a reflection has been carried out. It must be formalised in the data protection impact assessment when it is carried out.

4.2. Determine the qualifications of each stakeholder

Point of attention

The qualification of stakeholders must be carried out on a case-by-case basis. The examples below do not prejudge which qualifications could be retained in practice, taking into account each particular situation.

The supervisory authorities are not bound by the qualifications chosen by the parties, in particular within the contracts; it is possible for them to use a different classification depending on the circumstances of the case.

Qualifications of the publisher

In which cases can the application publisher be a controller?

Since it does not merely provide the software to the public but participates in its operation (e.g. data transfers between the user's terminal and its servers), the publisher of the application is responsible for the processing of the user's personal data carried out in the application, because it has determined the purposes and means of such processing, i.e. the purpose and manner of carrying them out (nature of the data collected, storage period, security requirements, etc.).

In particular, it shall be **responsible for:**

- **processing of personal data carried out in connection with the use of the application, for example:**
  - the user's account data (surname, first name, email address, telephone number, etc.);
  - the data necessary for the use of the services offered by the application (delivery address, bank details, discount card number, etc.).
- **the storage or gaining of access to information stored in the terminal operations he carries out on his behalf, as well as the processing of personal data resulting therefrom.** These include:
  - reading mobile identifiers for various purposes, for example:
    - reading of the mobile's unique advertising identifier in order to enable third-party advertisers to monitor user behaviour in the application;
    - reading by an application store provider[14] of the user's account identifier to personalise suggestions within the application store;
    - reading by the operating system provider[15] of the user's account identifier to track its activity to improve the functionality of the system mobile applications it makes available.
  - access to the various sensors on the mobile terminal (camera, location, etc.) when data is transmitted over a network for various purposes, for example:
    - reading the user's location to facilitate navigation within a route calculation application;

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

[14] The app store provider is understood here as the publisher of the mobile application that is the app store.

[15] The operating system provider is understood here as the publisher of the system mobile applications it makes available.

    - use of the camera sensor by an application to scan a QR code.
  - access to data stored on the mobile terminal (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 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.
- **storing and/or accessing operations carried out by third parties[16] (together with those third parties in the event that they jointly define the purposes and means of the processing).** For example:
  - reading of the unique advertising identifier of users by a third-party SDK for the purposes of advertising profiling on behalf of the publisher: the application publisher is responsible for the processing in relation to the operation (possibly jointly with the SDK provider);
  - reading of a technical identifier by a third-party SDK through the application on behalf of the third party to produce statistics for the purpose of improving its service: the publisher is jointly responsible for the processing.
- **storing and/or accessing operations carried out by third parties on its behalf and the processing resulting therefrom, which are also carried out by those third parties on its behalf.** For example, the application publisher is responsible for the operation carried out by the third-party SDK provider to read the unique advertising identifier and for the processing of users' advertising profiling carried out by the SDK provider on behalf of the publisher on the basis of that operation.

On the other hand, the publisher is not responsible for the processing carried out by third parties on their own account on personal data resulting from storing and/or acessing operations that they carry out through the application. Where the processing uses the data collected via the application, this collection must be provided for contractually between the publisher and the third party. For example:

- reading of a technical identifier by the third party to produce statistics for the purpose of improving its service: the publisher is not responsible for the statistical processing carried out by the third party;
- reading of the unique advertising identifier by the third party for the purposes of cross-referencing data with data from other applications to achieve its own advertising purposes: the publisher is not responsible for the data cross-referencing processing carried out by the third party.

Developer qualification

The publisher may have its application developed by an external developer. This raises the question of the developer's qualification under the GDPR.

Note: when the publisher develops its application internally, the publisher 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 application code and then no longer has any role in its operation or control over the personal data processed by the application, he is neither a controller nor a processor within the meaning of the GDPR.

However, the role of the developer is essential for the application to be designed in a way that respects the principles of the GDPR. In addition, while the responsibility for carrying out the data protection impact

[16] In the web environment, the responsibility for the processing of the publisher of a website was thus retained with regard to the access/storing operations carried out by third parties in a decision ' Éditions Croque Futur', No 412589 of 6 June 2018, in which the Council of State considers that the publisher of a site which authorises the deposit and use of third-party *cookies* must be regarded as the controller. Similarly, in deliberation No SAN-2021-013 of 27 July 2021, the CNIL considered that the publisher of the site had a certain responsibility (an obligation of means) with regard to the collection of consent on third-party *cookies*.
Thus, the fact that the *cookies* come from partners does not relieve the publisher of the site of its own responsibility in so far as it has control of its site and servers.

assessment lies with the controller, the security of the application is in practice based on the choices of the development provider. The CNIL therefore considers as good practices, in this configuration:

- that the contract between the developer and the publisher requires the latter to design an application allowing data to be processed in accordance with the GDPR, in a logic of data protection *by design (privacy by design);*
- that the publisher is involved in the structuring choices, including security, throughout the design of the application.

Providing an application that would, in itself, infringe the GDPR, entails the civil liability of the developer vis-à-vis the publisher.[17]

In which cases can the developer of the application be a processor?

The developer must be classified as a **processor if** it processes personal data on behalf of the publisher, who is responsible for the processing. This may be the case, for example, where:

- the developer implements the data processing and storage infrastructure;
- the developer performs operations on data hosted on the application server for the purposes of maintenance or outsourcing of the application.

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

By way of exception, the developer must be classified as **a controller separate** from the publisher if it processes data on its own account, for purposes it defines.

This may be the case, for example, where:

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

Where the developer intends to re-use the data entrusted to him in his capacity as processor for his own purposes, he must inform the publisher of the application of the purposes of that re-use and obtain his prior consent. The publisher will have to determine whether this further processing is compatible with the purpose for which the data were initially collected (Article 6-4 GDPR).

To go further

The CNIL has published a sheet on the re-use, by the processor, of the data entrusted by the controller.[18]

Qualification of the SDK provider

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

Often, exchanges of personal data take place between these stakeholders, which requires the SDK provider to identify and document its qualification, within the meaning of the GDPR.

In which cases can the SDK provider be a processor?

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

This is particularly the case where:

- the SDK performs storage or gaining of access to information stored in the terminal 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 with the aim of profiling it for advertising purposes on behalf of the publisher, by reading the terminal's unique advertising identifier;

[17] In particular, the contract between the publisher of the application and its developer may be declared void if failure to comply with the obligations of the contracting 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).

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

- the SDK analyses the user's location with the aim of profiling it on behalf of the publisher.

Where the developer of the application – who processes personal data on behalf of the publisher as a processor – uses an SDK provider to entrust it with part of the subcontracting operations, the latter must be regarded as a processor. Subsequent processors must provide the same level of guarantees as those offered by the initial processor vis-à-vis the controller.

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

The SDK provider is responsible for the processing of personal data carried out in the application for which it determines the purposes and means, i.e. the purpose and how to achieve them.

In particular, it shall be responsible for:

- **accessing and/or storing operations it performs (jointly with the publisher that allows this collection) if it retrieves data from these operations for its own purposes.** This may include, for example:
    - reading the unique advertising identifier for the purpose of user advertising profiling and for the purpose of improving the profiling service;
    - reading a technical identifier of the user's terminal for diagnostic and/or telemetry purposes of the application and for compiling statistics for the purpose of improving the SDK.
- **processing of personal data resulting from these operations.** The SDK provider is required to ensure that the application publisher is properly informed when carrying out such processing on its own account, in particular in the contractual elements it provides. This may include, for example:
    - the statistical processing that it carries out on the use of its service through the monitoring of users made possible by reading the technical identifier of their terminals, for the purpose of improving its service.

Qualification of the operating system provider

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

In many cases, the operating system provider is not involved in the processing of personal data within the applications.

The operating system provider is nevertheless responsible for the processing, 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 purposes and means.

These processing operations are largely independent of applications, but some are linked to them, in particular because they provide them with information and identifiers, some of which are personal data concerning the user.

The following situations need to be analysed to determine the qualification of the operating system provider:

- the local creation of a mobile identifier;
- 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, including application publishers. This applies in particular to 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 stakeholders (publishers, developers, SDKs) can only address one entity, Apple, regarding these issues. Moreover, there is currently no application store provider other 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) may approach different entities.[19]

[19] Thus, by way of example, at the date of adoption of these recommendations, an Android operating system will consist of:

- thus, these different entities are likely to share responsibilities depending on the data reuses that are made, in particular between Google, which may then have to **reuse data for its own account, and the manufacturers.**

Even when they are limited to providing technical tools without processing themselves, OS providers to some extent condition, through their technical choices, the way in which personal data processing is carried out by application publishers. **As such, OS providers are subject to certain good practices** (see Part 8 of these recommendations: ‘OS Provider Specific Recommendations’).

What role for the OS provider acting as a mobile application publisher?

The OS provider acting as the publisher of an application (such as system applications pre-installed within the OS and developed by itself) **is subject to the same qualifications and obligations as for any application publisher.** Thus, where the OS provider carries out processing of personal data for its own purposes within the applications that it develops and makes available within the OS, it must be classified as a controller.

What role for the OS provider acting as an SDK provider?

Similarly, the OS provider acting as an SDK provider is subject to the same qualifications and obligations as any SDK provider. Thus, when the OS provider carries out processing of personal data for its own purposes within the applications that it develops and makes available within the OS, it must be classified as a controller (if necessary jointly with the publisher).

Qualification of the application store provider

What role for the application store provider setting the rules for publishing apps?

The establishment of the rules relating to the application verification and validation procedure does not, in itself, involve the processing of personal data. Application stores therefore have no liability in that context within the **meaning of the GDPR.**[20] This does not exclude their liability in another way, in particular if the operation of the store leads them to process users’ IP addresses.

What role for the application store provider acting as a mobile app publisher?

The publisher of the store acting as an application publisher (the mobile application store itself being an application) **is subject to the same qualifications and obligations as any other application publisher.**

Thus, where the application store provider carries out processing of personal data for its own purposes (e.g.: processing of developer data in the context of application review processes before 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 is qualified as a controller.

Examples

An SDK provider accesses and processes a mobile identifier on behalf of the publisher and for its own account

An application publisher uses the services of an SDK provider to facilitate the development of its application. This introduces an SDK allowing access to the mobile’s unique advertising identifier to track user behaviour. If the user has given consent, the SDK queries the operating system to access the mobile’s advertising ID. The SDK measures the interactions between the user and the application through the tracking enabled by the identifier

- AOSP (Android Open Source Project: provision by Google of the code base of the Android operating system in open source*)*, Google Play Services and GMS (a software suite published by Google allowing access to other functionalities, including Google services (Chrome, Youtube, Gmail, etc.) for Google terminals; or
- AOSP, Google Play Services, GMS and a manufacturer suite (some manufacturers of multifunctional mobiles develop their own suites of applications intended to integrate the operating system of their terminals) for certain terminals (Samsung, Oppo, Nokia, Blackberry, OnePlus, Motorola, Xiaomi, etc.); or
- AOSP and a builder software suite for others (Huawei, Amazon, Murena, Fairphone, etc.), without the use of Google Play Services or GMS.

[20] The establishment by a co-contractor of contractual obligations having an influence on the processing of personal data carried out by its co-contractor is not sufficient to determine joint liability between them. It is necessary to determine whether, by means of those contractual obligations, the co-contractor influences, for his own purposes, the processing of personal data and thus determines the purposes of those operations and the means at the origin of those operations (CJEU, Case C-604/22, 7 March 2024).

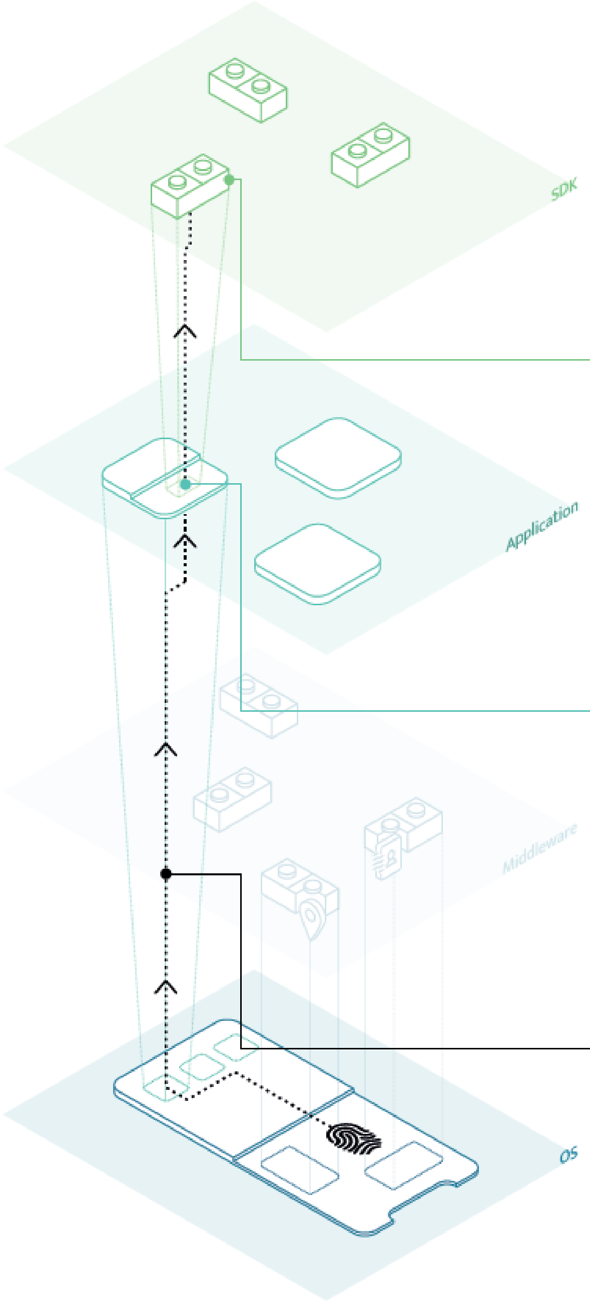
and carries out analyses on behalf of the publisher in order to allow it to know its audience and thus monetise the advertising spaces present in the application with advertisers. In this case, the SDK provider also wishes, with the contractual agreement of the publisher, to use the data collected for its own purposes, namely to improve its user profiling service for all its customers.

In this case:

- the publisher and the SDK provider are jointly responsible for the processing of access to the advertising identifier (which constitutes a reading and/or writing operation within the meaning of Article 82 of the French Data Protection Act) by the SDK provider because they participate jointly in determining the purposes and means of the processing concerning that operation;
- as regards the processing by the SDK provider, on behalf of the publisher (monetisation of advertising space in the application), of the personal data collected through access to that advertising identifier, the publisher is responsible for the processing and the SDK provider is its processor.
- the SDK provider may also process personal data collected through access to this advertising identifier for its own purposes, only if the publisher, who is responsible for the initial processing, has been properly informed and integrates the SDK with knowledge of the existence of such processing (for example via contractual elements). In this case, the SDK provider is responsible for its processing.

Reading and processing of a mobile identifier by an SDK on behalf of the publisher and on its own behalf

An application publisher uses the services of an SDK provider to facilitate the development of its application. The developer introduces an SDK into the application whose functionality is to access the unique advertising identifier of the mobile phone in order to be able to track the user's behaviour in the application.



SDK providers' purpose

Improvement of the user profiling service

Responsabilités

- The SDK provider is the data controller. It may only carry out this processing if this has been contractually agreed with the publisher.

Publisher's purpose

Monetisation of advertising space

Responsibilities

- The application publisher is the data controller
- The SDK supplier is a processor

Purposes determined jointly

Access to the advertising identifier

Responsibilities

- The application publisher is joint controller for the processing
- The SDK supplier is joint controller for the processing

An application accesses and processes location data via an SDK on the publisher's sole behalf

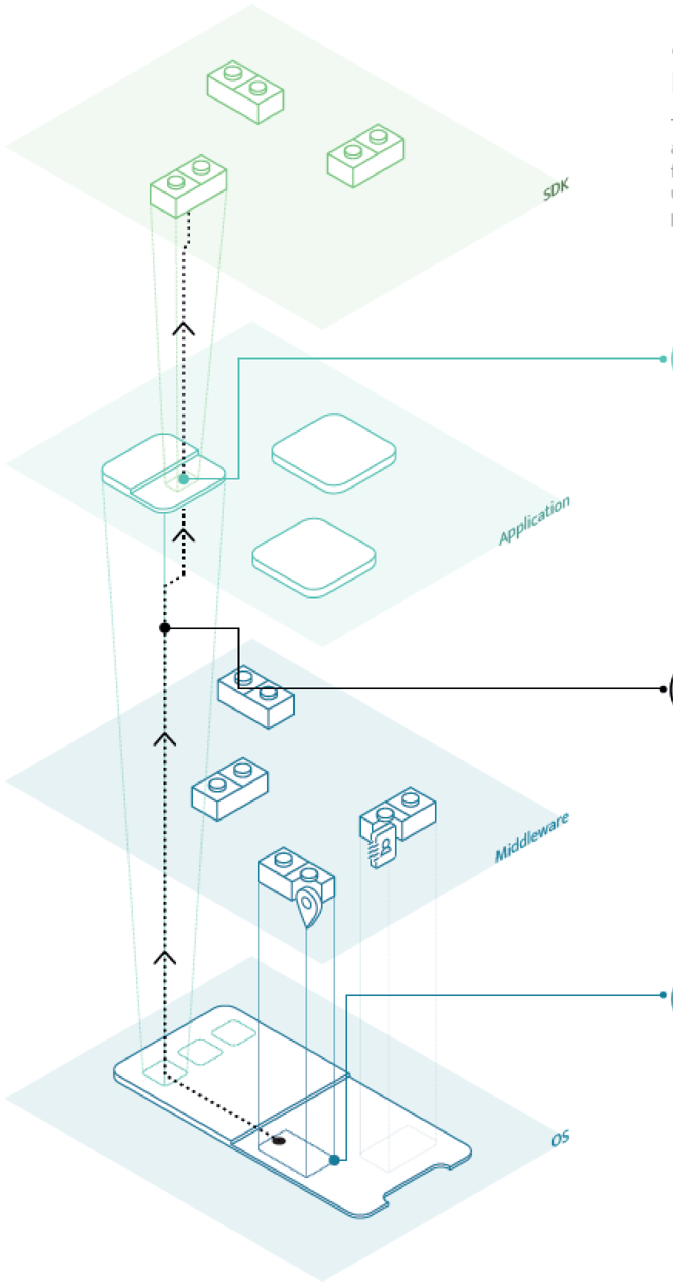
The publisher uses the services of an SDK provider to facilitate the development of the application. The functionality of this SDK is to access the user's location. This information is obtained by means of a precise location calculation service offered by the operating system provider on the basis of personal data to which it has access (IP address, lists of Wi-Fi access points and Bluetooth identifiers around the terminal). Access to location is for the benefit of both the user and the publisher. This allows the user to benefit from certain functionalities of the application (e.g. navigational aid, search for points of interest in the area). This also benefits the publisher: thus, the SDK provider uses that location information to carry out analyses on behalf of the publisher of the application in order to enable that publisher to know its audience and thus to monetise the advertising space present in the application with advertisers.

In this case:

- the publisher is responsible for the processing with regard to the inclusion within the application of an SDK whose function is to access location data (which constitutes a reading and/or writing operation within the meaning of Article 82 of the French Data Protection Act) ,and the SDK provider its processor because the SDK provider does not pursue any specific purpose here;
- as regards the processing by the SDK provider of the location data that it has collected on behalf of the publisher (audience awareness and monetisation of spaces), the publisher is responsible for the processing and the SDK provider its processor because the SDK provider does not pursue any specific purpose;
- the provider of the operating system is responsible for the processing it carries out for the purpose of offering the precise location calculation service to third parties, including in particular the publisher of the application.

Reading and processing of location data by an application via an SDK on the publisher's sole behalf

The publisher uses the services of an SDK to facilitate the development of the application. The developer introduces an SDK into the application, the function of which is to access the user's location. The location is obtained using a precise location calculation service offered by the operating system provider on the basis of personal data to which it has access.



Publisher's purpose

Monetisation of advertising space

Responsibilities

- The application publisher is the data controller
- The SDK supplier is a processor

Publisher's purpose

Access to location data

Responsibilities

- The application publisher is the data controller
- The SDK supplier is a processor

OS provider's purpose

Calculation and provision of precise location data

Responsibilities

- The operating system provider is the data controller

Accessing data from a contact book with transfer to the remote server of the application

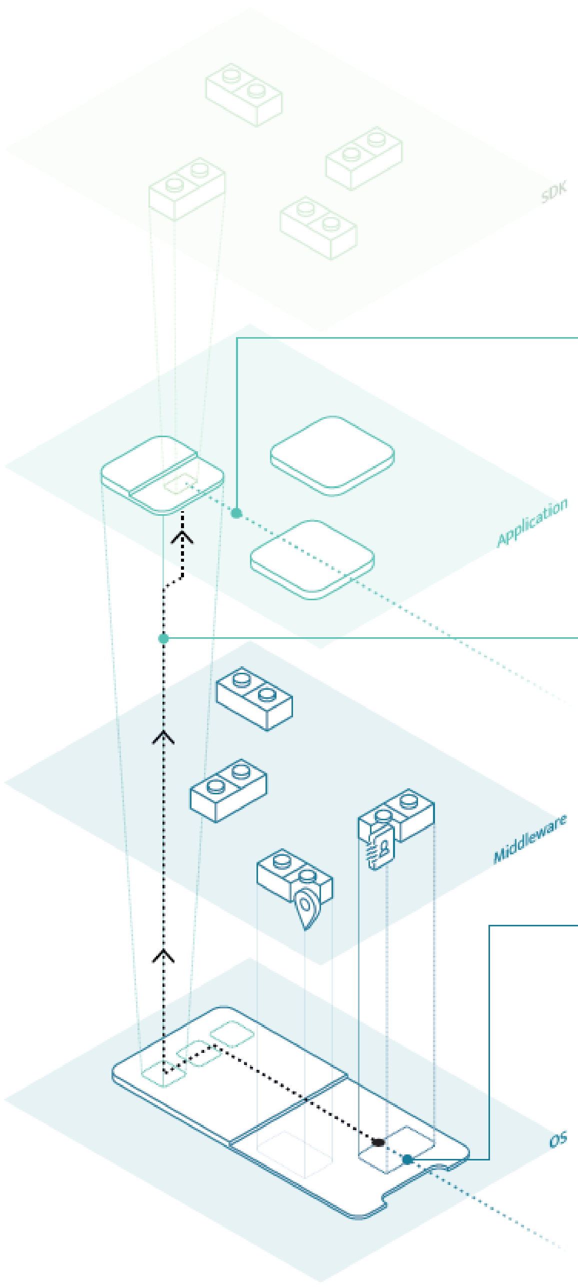
An application accesses data in a contact book, saved on the servers of the operating system provider, for application-specific purposes. This data is then transferred to the application publisher's server.

In this case:

- the operating system provider is responsible for the processing of the user's data stored on its servers;
- the publisher of the application is responsible for the processing with regard to access to such data (which constitutes a reading and/or writing operation within the meaning of Article 82 of the Data Protection Act) and for the processing of data subsequent to such access because it determines its purposes and means.

Reading data from a contact directory and transferring it to the application's remote server

An application accesses data from a contact directory for purposes specific to the application. The data resulting from this access is transferred to the application's remote server. This data is also saved on the operating system provider's servers.



Publisher's purpose

Provision of the service

Responsibilities

- The application publisher is the data controller

Publisher's purpose

Access to contact data

Responsibilities

- The application publisher is the data controller

OS provider's purpose

Saving contact data on its servers

Responsibilities

- The operating system provider is the data controller

References

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

5. Publisher-specific recommendations

How do I read this section?

This section recalls the obligations imposed by the laws (e.g. “the controller must”) and makes recommendations to comply with them (e.g. “the CNIL recommends”). It is possible for controllers to identify alternative ways of complying with obligations, but they must then be able to justify their choice and engage their responsibility. Some elements are also formulated as good practices and allow to go beyond compliance with the applicable laws (e.g. “As good practices, the CNIL encourages”).

Notice

To whom are these recommendations addressed?

- These recommendations are addressed to **application publishers.**
- The publisher of the application is defined as **the legal entity (or individual company of a natural person) that makes the application available to users** (most often through an application store) to offer its products or services.
- Obligations, recommendations and best practices apply to all publishers, including when they otherwise assume the role of OS providers or application store.
- These recommendations are addressed more specifically 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).

What is the purpose of these recommendations?

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

How can these recommendations be used?

- Each section corresponds to a stage in the provision of an application.
- Each thematic recommendation sets out the challenges of designing and operating an application in terms of the protection of personal data, recalls the main obligations stemming from the GDPR and the French Data Protection Act, and brings together a series of recommendations and best practices to be implemented.
- A **summary list of the main checks to be carried out** is proposed at the end of this section. Publishers are invited to refer to them, in particular when documenting their compliance.

See also

Publishers are also invited to consult, in this document, the recommendations applicable to other stakeholders, which may concern them, and in particular:

- Developer-specific recommendations
- SDK Provider Specific Recommendations

5.1. Design its application

As controller, the publisher must, where appropriate with the help of its partners, clearly define the processing of personal data carried out. It must take into account the protection of personal data from the design phase of applications.

1. Identify the existence of processing of personal data

The publisher must identify whether processing of personal data will be implemented through its application for the GDPR to apply.

- **Is it processing personal data?**
  - Personal data as defined in the GDPR is any information relating to an identified or identifiable natural person. For example: the surname and first name of the user, but also his alias, his geographical position, his activity data in the application or even the technical identifiers of the terminal he uses.
  - In some cases, applications may offer the requested service without processing personal data (e.g.: flashlight applications, virtual level indicator, compass, calculator, stopwatch or timer, metronome, tuner, some games, etc.)

- **Can the processing be exempted from the application of the GDPR?**
  - Under certain conditions (referred to in section 4 of these recommendations: 'What are the roles of each stakeholder in the use of the application?'),the processing falls within the domestic exemption, without entailing any liability of the application publisher within the meaning of the GDPR.

Point of attention

We must not forget to include in the analysis processing potentially carried out by third parties.

- **See section 5.2 of these recommendations: Mapping your partners**

2. Ensure compliance of personal data processing

The publisher must ensure that each of these personal data processing operations complies with the GDPR and the French Data Protection Act.

- **Is the purpose(s) of the data processing correctly defined?**
- **Is a legal basis identified for each purpose?** The publisher must identify a valid legal basis within the meaning of Article 6.1 GDPR for each of the purposes. Processing carried out in the context of mobile applications may in particular be based on consent, contract or legitimate interest:
  - Where the processing is based on consent, the publisher must ensure that consent is correctly collected (see section 5.3 of these recommendations: 'Managing consent and the rights of individuals').
  - Processing can only be based on the legal basis of the contract if it is objectively necessary for the contract entered into by the data subject. This means that it must be objectively indispensable in order to achieve a purpose that is an integral part of the contractual service provided to the data subject. The controller must therefore be able to demonstrate how the main object of the contract could not be achieved in the absence of the processing at issue and, therefore, that there are no practicable and less intrusive alternatives.
  - In order to rely on the legal basis of legitimate interest, the publisher must formalise an analysis of the balance of interests between the user whose data are processed and the controller. As recalled by the Article 29 Working Party, *'it would be difficult for controllers to justify using*

legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes. [21]

- **Is there storage or gaining of access to information stored on the user's terminal?**

  - The publisher must identify the storage or gaining access to information stored on the terminals of persons within the meaning of Article 82 of the Data Protection Act implemented on its applications. This includes, for example, access to mobile identifiers (whether of an advertising nature or not), results of fingerprinting operations, access to unique identifiers, such as hardware identifiers, access to telephone sensors or data stored in the terminal (contact book, photo gallery, etc.).
  - Consent is necessary for these operations unless they have the exclusive purpose of carrying out or facilitating electronic communication or are strictly necessary in order to provide an information society service explicitly requested by the user.
  - The CNIL recommends for this analysis be carried out by the publisher in conjunction with the developer so that precise instructions can be provided to him. For the CNIL's practical recommendations to enable the collection of consent in mobile applications, see section 6.2.3 of these recommendations ('Participating in compliance with the collection of consent').

[21] Opinion of the Article 29 Working Party on Profiling and Automated Decision-Making, WP 251, rev. 01 "it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering".

Read and/or write operations on the user's terminal are implemented				
By default: The consent of the person is required	**By way of exemption: the consent of the person is not required**			
Examples: • **collection of the advertising identifier for advertising purposes** • **collection of contact data for contact discovery purposes** • **collection of location for content recommendation purposes**	**The sole purpose of the storage or gaining of access to information stored in the terminal is to carry out or facilitate the transmission of a communication over an electronic communications network** Example: • use of identifiers for load balancing or routing purposes	**The operation is strictly necessary order to provide an information society service explicitly requested by the subscriber or user**		
		Functionality expressly requested by the user Examples: • access to GPS to provide a requested location feature • use of authentication identifiers (see use case 3.2 of the Guidelines on this subject[22])	**Use to secure the service, focusing on the protection of the user** (see use case 3.3 of the Guidelines on this subject[23]) Examples: • use of tracking devices to prevent denial of service attacks • use of tracking devices to prevent credential stuffing	**Limited audience measurement** Example: simple counting of the number of daily users for the purpose of sizing the service

- **Are the personal data processed limited to what is necessary for the purposes pursued (Article 5.1.c of the GDPR)?**

The publisher must ensure that the data collected for each purpose is limited to what is necessary for the intended purpose (e.g.: it is excluded to collect the full date of birth if the treatment only needs the year).

For some personal data, the publisher must in particular choose between the processing of technical data reported by the application or data provided manually by the user. For example, a meteorological application can use a location data manually filled in by the user or a location data retrieved by the terminal.

The CNIL recommends, whenever possible, giving preference to data provided manually by the user, who is thus in control of the data provided and its accuracy. It is important that all actors receiving this data for processing

[22] Opinion 04/2012 of the Article 29 Working Party on the exemption from the consent requirement for certain cookies, p. 7.

[23] Opinion 04/2012 of the Article 29 Working Party on the exemption from the consent requirement for certain cookies,p. 7.

(including possible third-party recipients of this data) are then aware that it is a data manually filled in by the user (this data then has the same status as a data filled in on a form of a website).

It is also recommended, where relevant, to give the user the choice between manually providing the relevant data or allowing the automatic transmission of data contained in their terminal.

- **Is the retention of data limited in time (Article 5(1)(e) of the GDPR)?**

The data processed must be kept for a period strictly necessary for the purpose of the processing.

- **Are sensitive data (political, religious, health, etc.) processed (Article 9 GDPR)?**
    - Such processing of sensitive data is prohibited unless it is based on one of the exceptions provided for in Article 9.2 of the GDPR, such as the free, specific, informed and unambiguous consent of the data subject.
    - Furthermore, any categorisation or creation of segments on the basis of such data for the purposes of advertising profiling is prohibited (Article 26 of Regulation No 2022/2065 on digital services, known as the 'Digital Services Act' or DSA).
    - If such processing is based on consent, it must be given prior to the processing of data and 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 be expressed in a specific way. To this end, the CNIL recommends displaying a warning or specific information before obtaining consent or adding a box to obtain separate consent.[24]

- **How to protect the data of minors?**

    - These recommendations do not specifically address the measures to be implemented in this respect; refer to the work published by the CNIL on the subject[25].
    - Minors benefit from special protections by law, additional measures must be implemented to protect their personal data and respect their privacy.
    - In addition, the dissemination of advertising based on profiling using personal data is prohibited where the recipient of the service is a minor (Article 28 of the Digital Services Act or DSA).

3. Apply the principles of data protection by design and by default (Article 25 GDPR)

The publisher must implement technical and organisational measures to protect personal data by design and by default ('data protection by design and by default' principles).

- **Are the application's default settings the least intrusive possible?**

    - It is recommended that the publisher determine, for each of the processing, the minimum parameters to provide the requested service (e.g.: it should not collect the person's location data by default if it only serves to facilitate the use of a search tool that can be functional without it).
    - To do this, the publisher should analyse these parameters in relation to each category of users (e.g.: the e-mail address of individuals should not be systematically collected if it is only useful for paying users in the context of invoicing).
    - If the publisher provides many services, it is recommended to allow the user to independently use each of the services offered.

- **Does the design of the system protect the privacy of users?**

[24] Paragraph 56 of Deliberation 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 is fully aware that his or her health data will be processed and sometimes stored by the controller, which in principle implies explicit information on this point when obtaining consent*'.

[25] "Digital rights of minors", cnil.fr

  - The publisher must analyse whether Privacy Enhancing Technologies *(PETs)* can be applied to the processing operations implemented.
  - For a review of some of these techniques and examples of use, the publisher may refer to the guides produced by the OECD[26] and the UK Data Protection Authority (ICO).[27]

- **Does this design minimise the risks for users?**

  - The publisher must minimise the data transmitted to its partners.
  - It is recommended not to transmit identifying data (name, alias, unique identifier number, etc.) if they are not necessary for the purposes pursued.
  - It is recommended that the publisher uses end-to-end encryption mechanisms to enhance data security.

4. Document its analysis (Articles 5.2 and 24 of the GDPR)

The principle of responsibility of actors obliges publishers to adopt tools and procedures to ensure the compliance of their processing on an ongoing basis. They must, in particular:

- **Maintain and keep up-to-date a record of processing activities (which is an obligation if the publisher is not exempted under Article 30.5 GDPR, and a recommendation otherwise).**
- **Justify and document the storage periods defined** according to the purposes pursued.
- **Conduct a data protection impact assessment (DPIA)** where the processing is likely to result in significant risks for data subjects.
- **Appoint a data protection officer where mandatory (incertain cases specified on the CNIL website).** In other cases, the CNIL recommends it.

5.2. Mapping partners

It is common for all or part of the data processing implemented to involve third parties. The publisher must therefore, as controller, have a complete view of the actors involved in the processing of data and the measures implemented by its partners to meet its obligations under Article 24(1) of the GDPR.

1. Supervise relations with developers

The publisher must supervise the relations with the technical partners he uses for the development of the application.

- **Is the qualification of the developer clear to both parties?**

  - The publisher must identify precisely and upstream the processing of personal data that will be carried out by the developer on the behalf of the publisher as part of the development and operation of the application. The developer then acts as the publisher's processor (see section 4 of these recommendations).
  - It must regulate the provision of subcontracting, for example via a data processing agreement (DPA), this qualification and the related obligations.
  - Warning: if the developer carries out processing operations on its own behalf, it may be classified as the controller for those operations (see section 4 of these recommendations, in particular: "Developer Qualification"). However, as the entity instructing the development of the application, the publisher must be informed of these processing operations and have accepted them, for example via the contractual elements.
  - The publisher remains potentially responsible for processing even if it does not take part in the development of the application. That is the case if it instructs a contractor to develop an application and participates in the determination of the purposes and means of the processing, even if it does not itself carry out the processing operations, does not expressly give its consent

[26] Emerging *privacy-enhancing technologies,* oecd-library.org
[27] Chapter 5: Privacy-enhancing technologies (PETs) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance (PDF, 722 KB), Sept. 2022, ico.org.uk

to the carrying out of the specific operations of such processing or to make available to the public the application and does not acquire that application. Thus, if the development process is interrupted along the way, it is necessary that the publisher explicitly opposes the publication of the application and the processing of personal data that would result. Otherwise, he would be regarded as a controller.[28]

- **Does the developer have the necessary elements to comply with his obligations?**
  - The publisher must provide clear instructions on the processing operations to be carried out, for example via the processor contract (Article 28(3)(a) GDPR).
  - It is recommended that the publisher:
    - set up a clear contact point for data protection issues (e.g. the Data Protection Officer);
    - provides clear and documented instructions in terms of security measures and compliance processes (see section 6.4 of these recommendations, in particular: 'Ensuring the security of the application');
    - provide in the contract for an acceptance test concerning compliance with these points.

2. Identify possible relationships with other third parties

If the developer is the publisher's main interlocutor in the development of an application, it is common for an application to involve data processing by other third parties.

- **While the publisher must be able to ensure compliance of all processing carried out by its processors,** this can be complex in the context of mobile applications, in particular as regards processing related to third-party SDKs, calls to OS APIs, performance analyses, battery use or telemetry carried out by OSs.
- **The CNIL recommends referring to Part 4 of these recommendations to identify all processing operations carried out by third parties as part of the conception and operation of the application.**
- The publisher may, as controller, require from all its processors, including where applicable the developer, a guarantee that the only processing carried out is that resulting from its documented instructions, pursuant to Article 28.3.1 of the GDPR.
- **The CNIL recommends that the publisher ask its developer to implement the SDK selection mechanisms described in section 6.3.1 of these recommendations ('Select the SDK according to the right criteria'),** since, as a controller, the publisher will assume at least co-responsibility for the use of tracking devices by an SDK included in its application.

5.3. Managing consent and people's rights

For processing operations for which it is responsible, the publisher must ensure that the rights of individuals are respected, whether in terms of information, consent or the exercise of other rights, even when their practical implementation depends on a third party.

1. Informing users correctly (Articles 12-14 GDPR)

To ensure transparency, and regardless of whether the data collection is direct or indirect, the publisher must properly inform users, for example in a 'privacy policy'.

- **What information should be provided to the users of the application whose data is being processed?**
  - This information must include:
    - the mandatory elements under Articles 13 or 14 of the GDPR[29];
    - the mandatory or optional nature of each processing operation (and, if applicable, how the refusal affects the use of the application).

[28] CJEU, Case C-683/21, 5 December 2023

[29] 'File No 12: Informing people",Development Team Guide , lincnil.github.io

- The CNIL also recommends including the list of permissions to access the data requested, their mandatory or optional nature and the purposes pursued via those permissions.

- The transmission of personal data of users to business partners, for example for the purposes of monetising the application, must be explicitly brought to the attention of individuals. If the processing operations in question require consent, the information given must be such as to enable the data subjects to assess the consequences of their choice by informing them of the extent of that choice. The CNIL recommends highlighting, among the data subjects, the number and the sector of activity of the partners who would be made recipients of the data.

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

  - The publisher must ensure that the privacy policy is easily accessible before any processing is implemented, directly from the application.
  - **The CNIL also recommends making it available before downloading the application, for example on its website or,** where possible, using the page dedicated to the application in the application store to:
    - provide the application's privacy policy;
    - indicate the main elements, in particular the identity of the publisher, the purposes of the processing operations and the manner in which the rights are to be exercised.
  - As a good practice, the CNIL encourages the presentation of permissions in two categories, depending on whether they only serve the service provided by the application to the user or also pursue other purposes.
  - The publisher must ensure that the privacy policy is concise, understandable by its audience using plain language.
  - The information can be carried out in several levels and accompanied by visual elements.
  - The use of a single privacy policy is not the only way to meet this information obligation, and may often, in the context of mobile applications, fail to achieve the objectives in terms of simplicity and conciseness: The CNIL recommends contextualising the information given during each specific collection and using simplified presentation methodologies in this case.[30]
  - As a good practice, the publisher may consider including specific information in the application interfaces on the access or sharing of certain particularly intrusive data (location, contact book, microphone, etc.), for example by displaying persistent indicators when these functionalities are enabled.

2. Obtaining valid consent from users (Articles 4 and 7 GDPR)

Consent may be necessary for storage or gaining of access to information stored in the terminal (Article 82 of the French Data Protection Act) or because it is the most appropriate legal basis for data processing (Article 6.1.a of the GDPR).

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

  - The CNIL guidelines and recommendation on *cookies* and other tracking devices[31] remain applicable to storage or gaining of access to information stored in the terminal in the context of mobile applications.
  - The CNIL recommends that the publisher take into account the specificities of the mobile interface, in particular the limitations in terms of available space.

Point of attention

- **As the publisher is responsible for collecting consent, it is recommended that it clearly explain its expectations to its developer and implement measures to ensure compliance with its instructions. To read the CNIL's practical recommendations to allow the**

[30] "[Synthesize] Summary", design.cnil.fr
[31] "Websites, *cookies* and other trackers", cnil.fr

collection of consent in mobile applications, refer to section 6.2.3 of these recommendations ("Take part to the compliance on consent collection").

3. Facilitating the exercise of rights (Articles 15-22 GDPR)

The publisher, who is responsible for the processing, must facilitate the exercise by users of their rights and ensure that they are respected.

- **What rights must the publisher respect?**
  - In general, the rights of individuals are the right of access, the right to erasure, the right to object, the right to portability, the right to rectification and the right to restriction of processing.[32]
  - Depending on the legal basis chosen, some of these rights are not applicable.[33]
- **What means should be made available to users and how should they be followed up?**
  - The texts do not impose specific arrangements to enable people to exercise their rights.
  - The CNIL recommends making available to users a rights management center within the application where all rights can be exercised. The publisher may ask its developer to advise it in this process.
  - The publisher responsible for processing must ensure that the replies provided to requests for the exercise of rights are complete, including with regard to the processing carried out by processors. Processors must implement appropriate technical and organisational measures to assist the publisher in responding to requests for the exercise of rights.
  - As a good practice, it can ensure that an automatic response is provided to users (e.g. via APIs for responding to requests for expressions of rights).

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

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

5.4. Maintain compliance throughout the lifecycle of the application

The publisher, as controller, must put in place a set of processes to ensure this compliance throughout the lifecycle of the application.

1. Ensuring the maintenance of security over time (Articles 32 to 34 GDPR)

The publisher must ensure the implementation of measures to ensure data security, in particular via the processor contract (Article 28(3)(c) of the GDPR).

The publisher must ask that processors send security alerts that may lead them to formalise a data breach notification (Article 33 of the GDPR) in compliance with the legal deadline for first notification (72 hours) to the data protection authority (in France, the CNIL).

In addition, the CNIL recommends:

- To formalise the expected technical measures in terms of data security with the developer (Article 32 GDPR), specifying that these requirements are applicable to sub-processors. The publisher may, for example, request compliance with the recommendations formalised by the CNIL in Part 6 of these recommendations ('Developer-specific recommendations');
- To ensure that the contract with the developer provides for the application to be updated in the event of a third-party vulnerability or in the code;
- To decouple important security updates (e.g. the correction of critical vulnerabilities), to make them available to users as soon as possible, from conventional functional updates (addition of new features).

2. Auditing compliance with partners' commitments

The publisher must implement sufficient and appropriate means to monitor compliance with its instructions by its processor (Article 28(1) GDPR).

- **How to implement audits?**
  - The publisher must provide in the processor contract that the developer allows audits to be carried out.
  - Due to the complexity of some applicative elements, the technical measures implemented alone are not sufficient to ensure compliance and must be complemented by organisational measures (see section 5.2 of these recommendations: 'Mapping partners').
  - As a good practice:
    - The publisher may use the *OWASP Mobile Application Security Testing Guide* (MASTG)[34] proposed by the NGO Open Web Application Security Project as a basis for analysing the security of its application.
    - The publisher can use a static analysis tool. These tools make it possible to verify that the included SDKs and the permissions requested correspond to its instructions. In case of doubt, the publisher can ask its developer to justify the observed elements (SDK included, permissions requested, etc.). Some tools offer more in-depth analyses, including security issues.
    - The publisher may set up (or engage a third-party provider for this purpose) a testbed to verify the proper functioning of the consent collection tools implemented. To this end, it may:
      - equip a test telephone or an emulator for interception of network communications;
      - test its application, and ensure that no symptomatic request for the use of tracking devices is made before consent is actually obtained.

[34] OWASP MASTG, mas.owasp.org

3. Implement robust processes in terms of compliance

Decisions that may impact the compliance of an application may be taken after the initial development of the application. In order to ensure continued compliance, the CNIL recommends designing and then implementing appropriate processes (on a regular basis or when significant development is undertaken).

- **Is the monitoring of possible developments in data processing well carried out?**
  - The publisher must update the record of processing activities to take account of developments in the data processing operations implemented, as well as the DPIA and the data privacy policy.
  - The CNIL recommends that the publisher set up a validation process in order to approve any changes in the conditions for implementing the processing (choice of a processor, SDK, functionalities, methods of obtaining consent) including when this occurs as part of a maintenance operation.

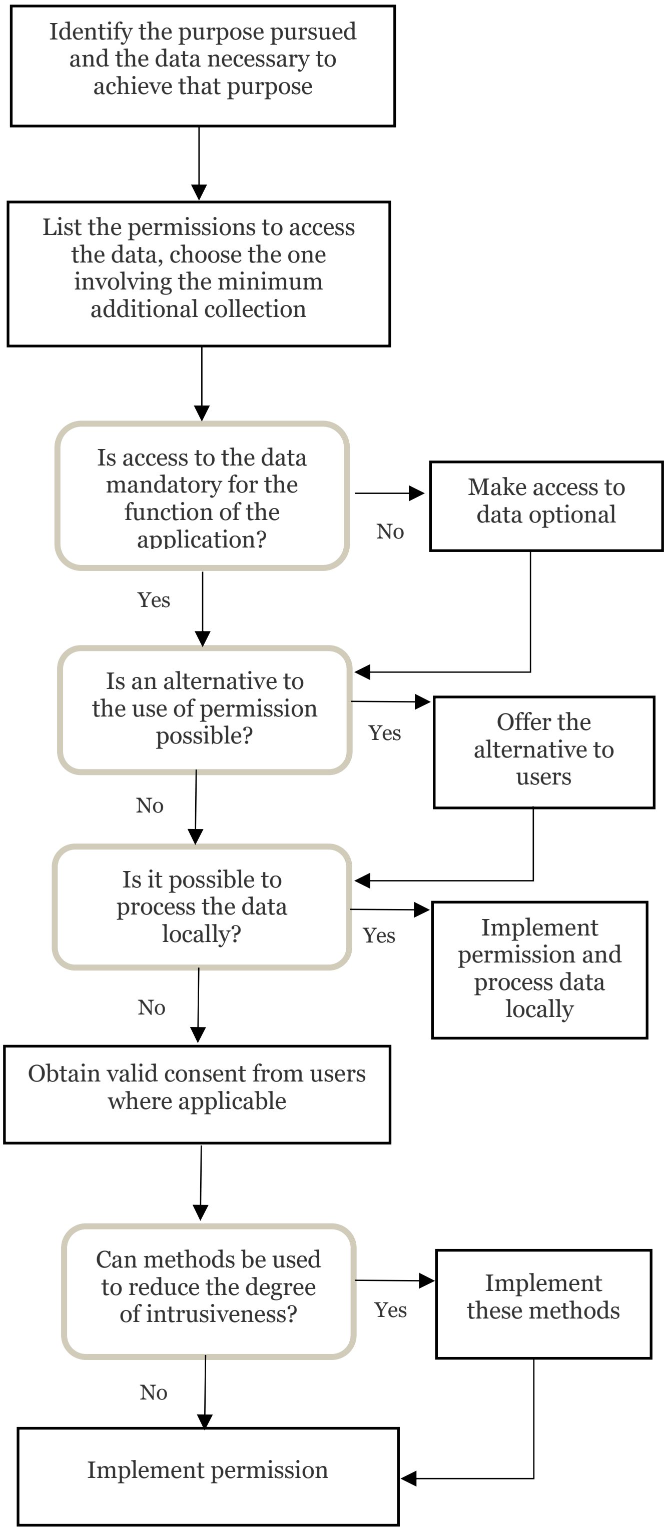
- **Are there processes in place to ensure the confidentiality of the data?**
  - The publisher must regulate the access to personal data by processors.
  - The CNIL recommends implementing logged access controls to avoid internal (personal or structural) abuse, as mentioned by the CNIL in its recommendation on logging[35]. The use of fictitious or synthetic data by processor is an alternative solution.
  - The CNIL recommends that the publisher supervises and verifies the deletion of data whose retention period has expired.

5.5. Permissions and data protection by design

Access to smartphone resources is often subject by OS to a permission system: the terminal user must allow their operating system to provide access to the edition to a certain type of data. The CNIL considers that the implementation of permission systems to give access to certain resources stored on the terminal (location, contact book, cameras and photographs/films, etc.) depending on the user's choice is a good practice, regardless of legal obligations.

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

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


Identify the purpose pursued and the data necessary to achieve that purpose
List the permissions to access the data, choose the one involving the minimum additional collection
Is access to the data mandatory for the function of the application?
No
Make access to data optional
Yes
Is an alternative to the use of permission possible?
Yes
Offer the alternative to users
No
Is it possible to process the data locally?
Yes
Implement permission and process data locally
No
Obtain valid consent from users where applicable
Can methods be used to reduce the degree of intrusiveness?
Yes
Implement these methods
No
Implement permission

1. Use permissions

How can permissions be analysed in the light of the applicable texts?

- Permissions in themselves are not intended to meet legal obligations and are an independent technical measure. However, remote access to a terminal resource following a permission request may be submitted to legal obligations:
  - Compliance with Article 82 of the French Data Protection Act and the GDPR. Article 82 requires prior consent, except where the storage or gaining of access to information stored in the terminal are necessary either for the carrying out of the electronic communication or for the provision of the service explicitely requested by the user. See section 5.3 of these recommendations 'Managing consent and the rights of individuals'.
  - Collection of consent under the GDPR.
  - Practical difficulties may arise in the relationship between these two types of consent (which can be merged) and permission (see section 6.2.3 of these recommendations: "Contribute to compliance with respect to the use of tracking devices and the collection of consent").
  - Where the permission relates to access to personal data, which is most often the case, the publisher must:
  - ensure that the person gives the permission in full knowledge of the facts and therefore has all the information necessary to understand why access to the data is requested. It is recommended to indicate clearly and intelligibly whether the functionality related to the permission sought is (i) necessary for the operation of the application, (ii) related to the activation of an ancillary function for the benefit of the user (facilitate its navigation, allow scanning a QR code, record a voice memo) or (iii) related to processing carried out for the benefit of the publisher or a third party separate from the provision of the service rendered by the application (advertising).
  - allow the user to consent separately where the purposes pursued are different (granularity of consent).
- The assessment of compliance with these principles is made globally (on the fact that publishers must be able to provide the necessary information when collecting permissions, and on the articulation of the different interfaces, see section 6.2.3 of these recommendations: "Take part to the compliance on consent collection", taking into account the principles of transparency and fairness which could, under certain conditions, render the collection of permission unlawful in particularly vague terms in order to guide the subsequent collection of more informed consent.

How to implement a permission selection process?

In the logic of data protection by design, the CNIL recommends implementing a permission selection procedure following the steps described in the diagram opposite.

2. Practical use cases for selecting permissions

How to manage the use of location?

- The publisher must identify on a case-by-case basis, among the permissions made available by the OS, the one enabling the objectives pursued to be achieved in compliance with the principle of minimisation:
  - an approximate rather than precise location,
  - permission limited to one time rather than permanent permission,
  - a permission that is only active when the application is in the foreground rather than permanently,
  - a permission that does not pass information on to third parties where possible (e.g. permission based on GPS alone and not network environment analysis).
- As a good practice, the publisher may propose an alternative to the use of this permission, for example the manual entry of a postal code or address instead of the processing of location data. It is recommended to clearly indicate that this is a data manually filled in by the user and not resulting from the operation of the system to the bodies that process it.
- The CNIL recommends that the publisher process the location data on the terminal. For example, in order to find the place closest to its user from a list of places, the CNIL recommends integrating the list in question into the content of the application and calculating on the terminal the nearest place according to the location of the person.
- Unless such collection is necessary to provide a service expressly requested by the user, the publisher must obtain valid consent for the remote collection of the person's location data.
- Before sending location data to the application's servers, the publisher must identify the minimum level of precision necessary to achieve its purposes and truncate the coordinates locally according to it, in accordance with the principle of minimisation.
- The CNIL recommends that the publisher do not keep the location data it has used on a remote server but rather keep it in the application, on the terminal, to offer it again to the user (via an item: "my last location").
- The CNIL recommends not collecting the location when the application is not actively used by the user.
- As a good practice, in case the permission given by the user is permanent, the publisher can remind him of the existence of the permission visibly in the interface of the application and ask him at regular intervals confirmation of his agreement to the location being collected.

How to manage access to contact data stored in the user's terminal?

- It is necessary to determine precisely the need for and the reasons for access to such contact data, and in particular whether such access is necessary for the operation of the application.
- The publisher must then identify the associated permission to pursue the purpose while respecting the principle of minimisation. For example, if a reading of the data is sufficient in view of the objective pursued, the publisher should not request writing rights.
- For any access permission involving the selection of a contact, it is recommended to make this selection directly on the user's terminal.
- If certain access permissions lead to the cross processing of contact data between several users of the application (for example, the discovery of contacts registered in a messenger, a mechanism that allows people to identify whether some of the people in their contact list are using the messenger they wish to use), the publisher must collect consent (Article 82 of the French Data Protection Act). It must inform all persons likely to be concerned by the

processing[36]. The publisher must ensure that the user is properly informed about the nature of the collection. As a good practice, it may propose alternative methods (e.g.: manual number entry by the person for spot check of presence) ensuring that these tools cannot be misused, e.g. by capping the number or frequency of possible queries to avoid multiple automated queries for scraping purposes.

- In a case where the publisher wishes to show the user the contacts who are already using the application in order to offer to connect it:
    - The CNIL recommends obtaining the consent of each user of the application to have their own contact details used in the future to be identified on third-party terminals or to be found by the accounts of third-party users who have their contact details;
        - Permission to access the telephone's 'contacts' must not be regarded as 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 be identified or searched be configured **by default** at the lowest possible level. The user would then have the choice between several settings options ('Only me', 'Friends', 'Friends of friends', 'All registered', 'Everyone, including non-registered', etc.).
    - The CNIL recommends using the most appropriate methods to limit the intrusiveness of access and the analysis of shared contacts (for example via 'Private *Set Intersection'* techniques).
    - The CNIL recommends deleting, at the end of the analysis, the contact data that would have been stored. It is recommended to set a limited duration of consent to access the terminal contacts for this purpose of comparison with the contact books of other users.

How to manage the use of the microphone?

- It is necessary to determine precisely the need and the reasons justifying access to the microphone, and in particular whether it is mandatory for the operation of the application.
- The publisher must identify the associated permission to pursue the purpose while respecting the principle of minimisation (in particular in terms of the possibility of collecting concurrent audio streams, which may pose a significant risk to the person).
- The CNIL recommends processing audio content locally: e.g. if a tuner is offered, the use of local phone computing capabilities should be preferred over remote content processing.
- Unless the use of the microphone is necessary to provide a service expressly requested by the user, the publisher must obtain valid consent for the remote collection of audio content, ensuring that the person understands that the content will be sent to its servers.
- In general, the CNIL recommends that sounds sent to a remote server should not be stored unless there is a specific and justified use. In particular, it recommends making the implementation of backups on a remote server optional, and to this end obtaining the free, specific and informed consent of users.
- Good practices include:
    - if the need is punctual, the publisher may revoke the permission after the sound has been recorded;
    - if the use of the microphone is only useful for certain actions in the application (e.g. recording a message), the publisher can alert the user when the microphone is activated, for example by means of a clearly identified and dedicated icon;
    - the publisher may offer its users to truncate or re-listen to the shared content before sending the audio content to the application's servers.

How to manage the use of the camera?

[36] 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) of the GDPR, the EDPS found not only a breach of Article 14 concerning the collection of data from non-users, but also that due to the invalidity of the anonymisation process used, that breach persists for the processing of data from non-users in the form of lists of non-users after applying the hashing procedure with loss.

- It is necessary to determine precisely the need and the reasons justifying access to the camera, and in particular whether it is mandatory for the operation of the application.
- The publisher must identify the associated permission to pursue the purpose while respecting the principle of minimisation. The CNIL recommends in particular:
  - Distinguish between access to the camera itself and access to photographs taken by the person and stored within their terminal if only one of the two is necessary.
  - to exclude the use of permissions requesting access to all the user's multimedia content if the processing does not require such full access in the light of the purposes it pursues. On the contrary, it must rely on permissions that enable the user to specifically select the content that he or she wishes to share with the application;
  - if this is not possible (e.g. for interactive uses of the video stream), require only the bare minimum in terms of hardware permissions (e.g. do not enable audio recording if not necessary).
  - in the event that a live photo or video recording is necessary, it is recommended that solutions delegating this recording to system applications be preferred;
- As a good practice, the publisher may propose an alternative that avoids access to the user's camera.
- The CNIL recommends processing the data on the terminal: for example, if the terminal offers editing tools, it is possible to consider the use of the phone's local computing capabilities rather than remote image processing. Similarly, it recommends deleting the metadata associated with the image (location, timestamp, EXIF data) if they are not necessary.
- Where the use of the camera is not necessary for the performance of a service expressly requested by the user, the publisher must in principle obtain valid consent for the remote collection of images, pursuant to Article 82 of the French Data Protection Law.
- Before sending images to its servers, the CNIL recommends analysing the need to obtain the entire image. Otherwise, it recommends offering selection or blurring tools to the user.
- In general, the CNIL recommends not to store the images sent to a remote server unless there is a specific and justified use. In particular, it recommends making the implementation of backups on a remote server optional and that the default setting does not include this backup.

5.6. Checklist

These verifications are intended to guide publishers in the implementation of these recommendations and are presented as an indication. Some of the checks to be carried out may correspond to good practices or recommendations and not to obligations: in case of doubt, refer to the text of the recommendation.

Category	Subcategory	Identifier	Description
Design its application	Identify the existence of processing of personal data	1.1.1	All personal data and related processing operations are identified
	Ensure legal compliance of processing operations	1.2.1	Each processing carried out has an identified legal basis.
		1.2.2	Storage or gaining of access to information stored on the terminals of the persons implemented within the applications are identified.
		1.2.3	No unnecessary data collection is carried out. Necessary ones are minimized.

		1.2.4	A data retention period is associated with each processing.
		1.2.5	Sensitive data processed are identified.
		1.2.6	Additional measures are applied to the data of minors.
	Apply the principles of data protection by design and by default (Article 25 GDPR)	1.3.1	The list of minimum parameters to provide the requested service is determined and is offered by default.
		1.3.2	These parameters are analysed in the light of the different categories of users.
		1.3.3	The possibility of integrating privacy mechanisms is explored from the design stage.
	Document its analysis (Articles 5.2 and 24 of the GDPR)	1.4.1	A record of processing activities is carried out.
		1.4.2	Retention periods are justified and documented.
		1.4.3	A DPIA is carried out if the processing meets the criteria.
		1.4.4	A data protection officer are appointed within the publisher.
Mapping partners	Supervise relations with developers	2.1.1	The qualification of the developer is 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 instructions given to the developer on the processing to be implemented are clear and documented, and a point of contact dedicated to privacy issues is made available to him.
	Identify possible relationships with other third parties	2.2.1	All third parties involved in the application are analysed to identify whether they are processing personal data.
		2.2.2	Any implemented SDK is analysed with the potential help of the developer to identify whether it is processing personal data.
Managing consent and people's rights	Informing users correctly (Articles 12-14 GDPR)	3.1.1	A complete privacy policy, concise and understandable by its public is drafted.
		3.1.2	The privacy policy is accessible before any downloading of the application, for example on the download page of the application. The privacy policy is also accessible within the application.
	Obtaining valid consent from users (Articles 4 and 7 GDPR)	3.2.1	The obligations in terms of collection of consent as explained by the CNIL in its guidelines and recommendations on *cookies* and other tracking devices are implemented.

	Facilitating the exercise of rights (Articles 15-22 GDPR)	3.3.1	An analysis is carried out on the rights applicable to individuals (right of access, right to portability, right to restriction, etc.).
		3.3.2	A rights management centre is set up directly within the application.
Maintain compliance throughout the lifecycle of the application	Ensuring the maintenance of security over time (Articles 32 to 34 GDPR)	4.1.1	The requirements in terms of expected technical measures are formalised with processors.
		4.1.2	The obligations in terms of a security alert to allow the notification of personal data breaches are reminded to processors.
		4.1.3	The process of updating in case of vulnerability is contractualized with third parties.
	Auditing compliance with partners' commitments	4.2.1	If the risks so warrant, audits are carried out on processors to verify compliance with the instructions given.
	Implement robust processes in terms of compliance	4.3.1	The updates are reflected in the record of processing activities, in the DPIA and in the privacy policy.
		4.3.2	Instructions are given to processors so that any evolution impacting privacy issues is approved before implementation.
		4.3.3	Personal data is protected and access to it is logged to prevent misuse.
		4.3.4	The deletion of data whose duration has expired is organized.
Permissions and data protection by design	Use permissions	5.1.1	For each data that is required to be collected, the permission that involves the least amount of additional data collection is chosen.
		5.1.2	Alternatives to the use of permissions are offered to individuals where possible.
		5.1.3	The data collected is processed locally where possible.
		5.1.4	Consent is validly collected where necessary (see 3.2.1).
		5.1.5	Before any remote collection, the accuracy of the data is reduced to the minimum necessary.

6. Developer-specific recommendations

How do I read this section?

This section recalls the obligations imposed by the law (e.g. "the controller must") and makes recommendations to comply with them (e.g. "the CNIL recommends"). It is possible for controllers to identify alternative ways of complying with obligations, but they must then be able to justify their choice and engage their responsibility. Some elements are also formulated as good practices and allow to go beyond compliance with the law (e.g. "As good practices, the CNIL encourages").

Notice

To whom are these recommendations addressed?

- These recommendations are addressed to **application developers.**
- The developer of the application is defined as **the legal entity or individual company that carries out the technical operations of the development of the application, on behalf and at the direction of the publisher.**
- Obligations, recommendations and best practices apply to all developers, including when they otherwise assume the role of publisher, SDK provider, OS or application store. In particular, in case the developer and the publisher are a single entity, it will have to consult both the recommendations applicable to the publisher and the developer.
- These recommendations are addressed more specifically to the developer:
  - the Data *Protection Officer* (DPO) of an application development agency;
  - project managers responsible for developing applications;
  - members of the application development team.
- These recommendations can also be consulted by any developer partner 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 may have a strong impact on the processing of personal data that will be implemented by the publisher.
- It must therefore implement an approach to ensure that the publisher is informed and validated of the technical choices made and their implications and thus complies with its duty to advise. **These recommendations are intended to help the developer in this process, throughout its development and maintenance of the application.**

How can these recommendations be used?

- Each section corresponds to a stage in the development activity of an application and sets out the privacy issues and brings together a series of recommendations and best practices to be implemented by developers.
- A **summary list of the main checks to be carried out** is proposed at the end of this section. Developers are invited to refer to it, in particular when drafting their documentation in order to assess the level of consideration of CNIL recommendations by their partners.

See also

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

- Publisher-specific recommendations
- SDK Provider Specific Recommendations

6.1. Formalise your relationship with the publisher

Note that if only direct relationships between publishers and developers are dealt with here, the use of sub-processors (e.g. providers hired by developers) will require the cascading consideration of these recommendations.

1. Identify the responsibilities and obligations of each

The contract between the controller (publisher) and the processor[37] (developer) must define the responsibilities of each.

- **Is the developer a processor within the meaning of the GDPR?**
  - The developer must be qualified as a processor if he is involved in the processing of personal data on behalf of and at the instruction of the controller.
  - As a reminder, the fact that the developer makes certain technical choices does not necessarily make him a controller: a processor may determine the non-essential means of a processing operation[38].
  - The CNIL recommends the developer to refer to part 4 of these recommendations to determine its qualification under the GDPR.
- **What requests should be made to the publisher?**
  - When contracting with the publisher, the developer is recommended to ask the publisher for an explicit qualification of its role for each of the processing operations concerned.
  - When subcontracting, the developer must ask the publisher to provide, in the specifications, instructions on the processing operations to be carried out, making it possible to define which data will be used.
  - The processor contract must provide in this case that the developer must limit the processing carried out to the instructions provided (Article 28 GDPR).
  - The CNIL recommends that the contract include a contact point to validate the choices having an impact on the processing of personal data: this may be the publisher's data protection officer.
- **What are the obligations on the developer's side?**
  - When acting as a processor, the developer must comply with a number of obligations (Article 28 GDPR) and in particular:
    - an obligation of transparency and traceability. As a good practice, the developer could thus make the source code of the application available to the publisher;
    - the obligation to assist its client, the publisher, in compliance with its obligations in terms of responding to the exercise of rights under the GDPR (see section 6.2 of these recommendations, 'Assume its advisory role towards the publisher');
    - the obligation to guarantee the security of the data processed (see section 6.4 of these recommendations 'Ensuring the security of the application').
    - the obligation to alert the publisher if the instructions provided do not comply with the GDPR, in particular in terms of compliance with the principles of data protection by design and by default;
  - The processor developer must keep a record of the processing activities carried out on behalf of the publisher subject to the conditions laid down in Article 30.3 of the GDPR.
  - The subcontracting developer must ensure that the personal data it collects and processes on the instructions of the publisher correspond to those of the record of processing activities or the exhaustive specifications communicated by the publisher. Otherwise, it is recommended to alert the publisher so that this document is updated.

[37] 'Data controller and processor: 6 Best Practices for Respecting Personal Data",cnil.fr
[38] EDPS Guidelines 07/2020 on the concepts of controller and processor (PDF, 1.6 MB), edpb.europa.eu

- In all cases, the developer must act on documented instructions from the controller, validating the possible use of sub-processors in accordance with Article 28 GDPR.
- If sub-processors recruited by the processor developer carry out storage or gaining of access to information stored in the terminal on their behalf, they may be responsible or jointly responsible for the processing with the publisher concerning these operations (see section 4 of these recommendations: 'What are the roles of each stakeholder in the use of the application?): the use of these service providers and their qualification within the meaning of the GDPR and the ePrivacy Directive must be validated by the publisher.
- Finally, with regard to developer-specific environments (e.g.: technical environment for shared development between its customers):
  - If the developer carries out data processing on its own account, it must, where applicable, comply with all the obligations of a controller. This can be the case especially if test data is used for the different applications developed by the developer.
  - The developer only carries out processing reusing the data it holds as a processor, for its own purposes, with the prior consent of the publisher and provided that the processing is compatible with the original purposes, in accordance with Article 6-4 GDPR[39] (see Part 4 of these recommendations, 'What are the roles of each stakeholder in the use of the application?').

2. Implement project management processes agreed by both parties

What decision-making process?

- If a decision impacting the privacy of users (technical choice, interface design, etc.) is identified by the developer, the CNIL recommends not taking this decision alone but, on the contrary, involving the publisher in the decision-making process.
- The CNIL recommends that the contact point identified within the publisher for this purpose be used to facilitate communication. It recommends that the developer also identify a contact person for any questions relating to data protection issues (e.g. if there is a DPO for the structure).
- The CNIL recommends presenting the issues clearly and asking for written instructions to be sent to it, in order to be able to demonstrate that it is acting on instructions from the controller.
- The CNIL recommends paying particular attention to the following subjects:
  - 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 the event of refusal;
  - choice of arrangements for any collection of users' consent;
  - informing users and exercising their rights.

What processes to ensure the compliance of personal data processing in the long term?

- The CNIL recommends maintaining the decision-making process described above throughout the lifetime of the application, in particular following an external evolution or an alert (e.g.: update of an SDK, detection of a security breach). In these situations, it recommends proactively informing the publisher. Some tools can help the developer analyse updates to partners' terms of use.
- As a good practice, if changes in the permissions proposed by the OS make it possible to better protect people, the developer may suggest an update to the publisher.

[39] 'Processors: the reuse of data entrusted by a data controller", cnil.fr

- **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, this is often done in practice by the developer, in particular as a result of technical restrictions imposed by application store providers.
    - As a good practice, the developer can ensure that he has all the elements required to ensure that users in these stores are properly informed and, if not, can ask the publisher to send them to him.
    - The app upload account must be secure, excluding any password sharing.
    - If the developer is instructed to distribute the application without going through an application store, he must ensure that he has the ability to guarantee the integrity of the distributed content.

3. Identify all processing of personal data

While the majority of processing will be listed in the record of processing activities provided by the publisher or in an exhaustive specification, certain development choices may involve the implementation of additional processing. The CNIL recommends that the developer inform the publisher of the existence of processing of personal data and, in conjunction with the publisher, determine the associated responsibilities.

- **Does the use of functionalities made available by the OS involve the processing of personal data?**
    - The processor developer must analyse, when using tools provided by the OS, whether their use involves the processing of personal data.
    - For example, when using data backup functionalities (sometimes enabled by default), it must inform and assist the publisher in the qualification of this processing and related issues (e.g. in relation to data transfers outside the European Union, within the meaning of Chapter V of the GDPR[40]).
    - It must analyse in this way all the APIs provided by the OS (notification, payment, *single sign-on,* system health monitoring, security, fault management, etc.) to ensure that it does not implement processing without instructions from its controller.
    - The CNIL recommends to follow the evolutions of the OS and their functionalities, in particular in terms of minimization of the processed data.

- **Are processing implemented as a result of SDK integration?**
    - The processor developer must analyse, when using SDKs, whether the use of SDKs involves the processing of personal data (e.g. the collection of a unique hardware identifier, the collection of IP addresses, surrounding Wi-Fi identifiers, etc.).
    - If this is the case, it is recommended that it obtain information on the characteristics of the processing in order to qualify those third parties within the meaning of the GDPR. As such, it can refer to Part 4 of these recommendations ("What are the roles of each stakeholder in the use of the application?").
    - The CNIL recommends collecting for this purpose the list of personal data collected, the object, nature and purpose of the processing carried out on these data according to the configuration of the chosen tool. In the absence of these elements, if doubts remain about the processing actually involved in the use of the SDK, the CNIL recommends that the developer inform the publisher and consider renouncing the use of the SDK. In particular, if the processor developer considers that processing carried out following the integration of the SDK infringes the GDPR, it has an obligation to inform the controller thereof.
    - This analysis should be applied to all SDKs used, including those provided by the OS provider.

6.2. Assume its advisory role towards the publisher

The developer, when it is a processor within the meaning of the GDPR, must assist and advise the publisher in its compliance with certain obligations laid down by the GDPR, particularly as regards respect for the rights of individuals and the security measures to be implemented (Articles 28(3)(e) and 28(3)(f) of the GDPR). It also has an obligation to inform it if it considers that an instruction given by it infringes the GDPR. The CNIL

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

recommends that the developer ensure that the controller is informed of the technical choices made and their implications, for which the developer is contractually liable[41].

1. Helping to ensure that users' rights are properly respected

If the developer is a processor, he must assist the controller in order to ensure that the rights of individuals are respected (Article 28(3)(e) GDPR). It can, as a good practice, ensure, when designing the application, that the rights can indeed be exercised effectively within the application regardless of its classification.

- **Is it possible to exercise rights within the application?**
  - The processor developer must take technical and organisational measures to enable the exercise of rights, in particular in terms of structuring databases. For example, the right of deletion must be respected, regardless of technical constraints.
  - The CNIL recommends 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 allows the publisher to avoid collecting additional data to fulfil the exercise of the rights, by simply making use of the identifiers used for the collection in order to implement it.
  - The developer must ensure that, when the rights of access or portability are exercised, all the data concerned are transmitted to the person. This requires, if processing is carried out by third parties such as SDKs and the publisher wishes to provide an automatic response to requests, that those third parties provide rights management APIs in order to make it possible to automate the process.
- **Are users well informed?**
  - As a good practice, the developer can remind the publisher of the need to make available the privacy policy that the latter provides within the application.
  - In addition, a data protection information screen may be made available at the first launch of the application.

2. Propose developments respecting the principles of personal data protection

- **Is the principle of data minimisation taken into account?**
  - The developer, as a processor, must ensure that the processing operations it carries out on behalf of the publisher comply with the instructions given by the publisher, in particular as regards the principle of minimisation of the data collected.
  - As such, if the developer identifies that certain data is accessible by third parties (the OS or an SDK, for example), the CNIL recommends proposing solutions to limit the risks associated with such access and in particular:
    - limit the data displayed in the notifications issued by the application, by simply indicating that these are available within the application. When possible, encrypt the content of the notifications, so that the OS provider is not able to access them;
    - encrypt the contents of the backups, allowing the user of the application and them alone to retain control of the cryptographic keys used for this encryption;
    - avoid the transmission of inter-application identifiers to SDK providers. If this transmission is necessary, perform a hash of the identifiers.
  - In the event that the developer has to implement web browsing functionalities within the application, the CNIL recommends ensuring that they do not allow more data to be collected than when browsing using web browsers. It recommends respecting the preferences and settings of the terminal using the web browser chosen by the user.
  - If the developer does not have specific instructions concerning the permissions to be collected, he must ensure that the ones he will ask for correspond to the publisher's expectations.
  - The CNIL recommends ensuring that the permissions requested are necessary for the operation of the application and the purposes of the processing, and advising the publisher on ways to minimise the collection authorised according to the permission levels. Where possible, the CNIL recommends proposing alternative and voluntary data collection methods on the part of

[41] In particular, the contract between the publisher of the application and its developer may be declared void if failure to comply with the obligations of the contracting 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 user in the event of refusal (see section 5.5 of these recommendations: 'Permissions and data protection by design') For the most intrusive permissions, the developer may, as a good practice, propose to notify the user when they are active, via the OS functionalities or within the application.

- The developer must ensure that the use of permissions is compatible with the publisher's instructions regarding the need to obtain valid consent before any reading and/or writing operation, in conjunction with the publisher (see section 6.2.3 of these recommendations: "Participate in compliance with the collection of consent"). The CNIL recommends limiting the use of block permissions to the installation as much as possible ('*install-time permissions'),* preferring the use of permissions that can be triggered during the operation of the application ('*runtime permissions*').
- As a good practice:
  - The developer can technically advise the publisher to choose and implement more protective solutions. The CNIL encourages:
    - the use of privacy protection techniques (e.g. as described in a guide on the subject produced by the ICO[42]);
    - the use of methods to perform data operations and calculations locally within the terminal, instead of using remote APIs.
  - The developer may analyse the publisher's instructions to identify whether the data it is asked to process is indeed necessary, and, if not, offer to exclude certain data from the processing.

- **Does the processing involve sensitive data within the meaning of Article 9 GDPR?**

For the definition of sensitive data within the meaning of Article 9 of the GDPR: see section 5.1 of these recommendations: Ensuring legal compliance of processing operations

- The developer may process sensitive data only after having received explicit instructions to that effect from the publisher (Article 28(3)(a) GDPR). Failing that, it must inform the publisher if it identifies processing of sensitive data so that the latter can analyse the compliance of the processing and modify its instructions.
- The publisher must be alerted in the event of irrelevant or even unlawful use of sensitive data, either by design or by mistake (e.g.: use of sensitive data to target advertisements) under Article 28 GDPR. As a reminder, any categorisation or creation of segments on the basis of such data for the purposes of advertising profiling is prohibited (Article 26 of Regulation No 2022/2065 on digital services, known as 'Digital *Services Act'* or DSA).
- Particular attention must be paid to the processing of such data, in particular in the case of transmission to third parties. For example, when integrating SDK, the CNIL recommends that the developer ensure that they have no access to this data.
- If the instructions provided by the publisher involve the processing of sensitive data, the CNIL recommends that the developer make a clear distinction between these and other data typologies, particularly in terms of the architecture of the service.

3. Participate in compliance with the collection of consent

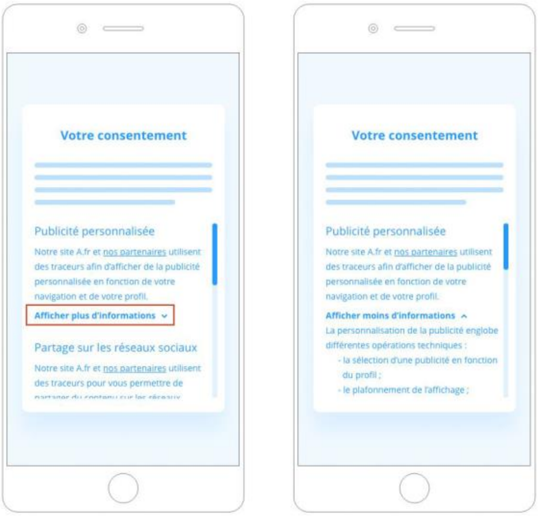
The CNIL recommends that the developer alert the publisher if elements of the specifications involve the collection of consent (pursuant to Article 82 of the French Data Protection Act or the GDPR) and, as far as possible, participate in the proper implementation of that consent. For more details on the contexts in which consent may be required, see section 5.1.2 of the Recommendations to Publishers.

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

- The guidelines and recommendation "Cookies and other tracking devices" published by the CNIL are relevant in the context of mobile applications.

[42] Chapter 5: Privacy-enhancing technologies (PETs) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance (PDF, 722 KB), Sept. 2022, ico.org.uk

- Interfaces need to be adapted to make windows legible in a mobile environment. The CNIL recommends paying particular attention to accessibility issues to enable everyone to provide valid consent.



Votre consentement

Publicité personnalisée

Notre site A.fr et nos partenaires utilisent des traceurs afin d'afficher de la publicité personnalisée en fonction de votre navigation et de votre profil.

Partage sur les réseaux sociaux

Notre site A.fr et nos partenaires utilisent des traceurs pour vous permettre de partager du contenu sur les réseaux

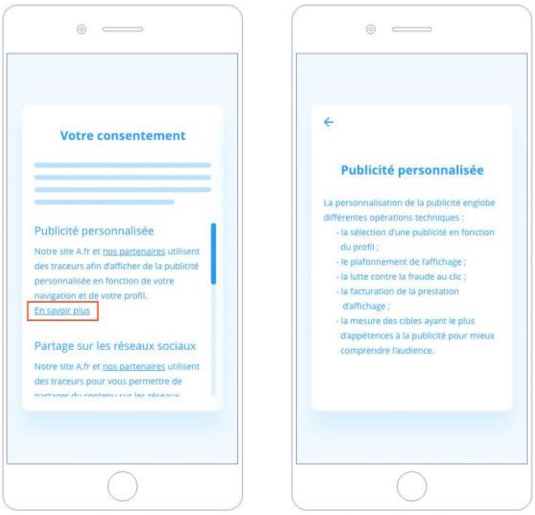
Votre consentement

Publicité personnalisée

Notre site A.fr et nos partenaires utilisent des traceurs afin d'afficher de la publicité personnalisée en fonction de votre navigation et de votre profil.

La personnalisation de la publicité englobe différentes opérations techniques :
- la sélection d'une publicité en fonction du profil ;
- le plafonnement de l'affichage ;

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



Votre consentement

Publicité personnalisée

Notre site A.fr et nos partenaires utilisent des traceurs afin d'afficher de la publicité personnalisée en fonction de votre navigation et de votre profil.

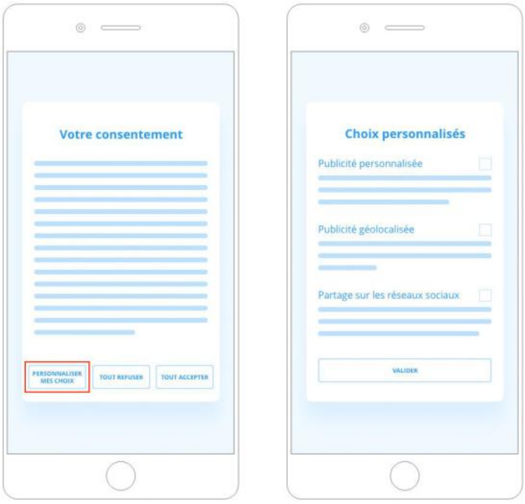
Partage sur les réseaux sociaux

Notre site A.fr et nos partenaires utilisent des traceurs pour vous permettre de partager du contenu sur les réseaux

Publicité personnalisée

La personnalisation de la publicité englobe différentes opérations techniques :
- la sélection d'une publicité en fonction du profil ;
- le plafonnement de l'affichage ;
- la lutte contre la fraude au clic ;
- la facturation de la prestation d'affichage ;
- la mesure des cibles ayant le plus d'appétences à la publicité pour mieux comprendre l'audience.

Figure 2 - Details of the purposes are available by clicking on a hyperlink on the first level of information



Votre consentement

Choix personnalisés

Publicité personnalisée □

Publicité géolocalisée □

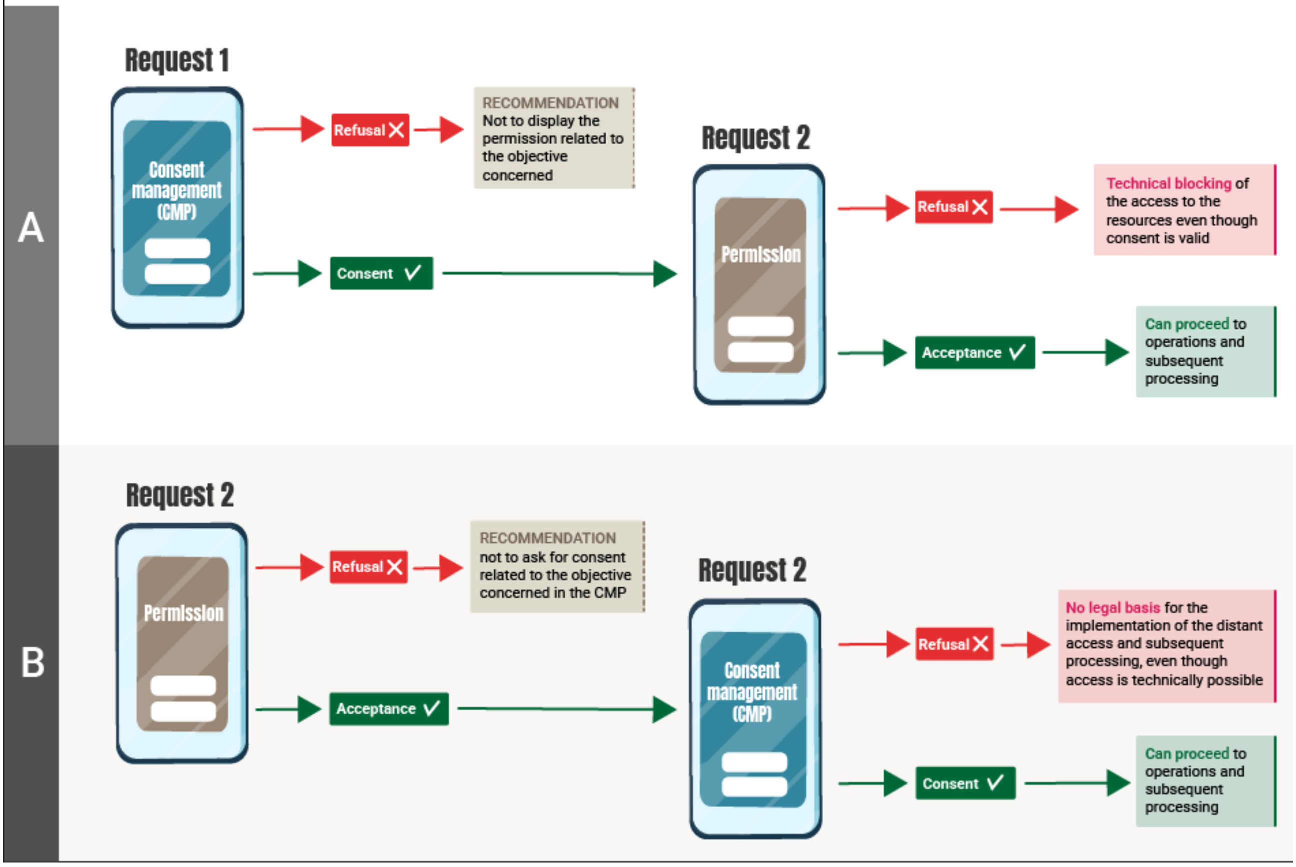
Partage sur les réseaux sociaux □

Figure 3 - The possibility of consenting granularly may be offered on a second level of information via a button 'customise my choices' inserted on the same level of information (first level) as the buttons for 'accepting everything' and 'refusing everything'.

- The CNIL recommends agreeing on the arrangements for obtaining consent upstream with the publisher and putting them in place within the application on the basis of its instructions, documenting this approach.
- To reduce fatigue in the face of excessively long requests and to make the collection of consent more understandable for users, the CNIL recommends, as a good practice, to collect consents in a contextual manner according to the actions taken instead of a single initial screen.

- **How to articulate the collection of consent and permissions?**
  - In general, obtaining these permissions makes it possible to give technical access to the resource in question. However, the request for permission does not necessarily lead to a valid consent under the GDPR or Article 82 of the French Data Protection Act.
  - The developer is recommended to agree with the publisher on the need to implement a *Consent Management Platform* (CMP) in addition to the permission window.
  - Consent may be obtained either before or after the request for permission. The CNIL recommends that the developer, in conjunction with the publisher, choose the method that is easiest for the user to understand (for example by emulating or annotating the permissions interface), avoiding soliciting it unnecessarily (see the table below): the user should have the relevant information to understand what they are giving access to and why as early as possible in the process of obtaining their authorisation.

COORDINATING THE TECHNICAL PERMISSION WITH THE CONSENT MANAGEMENT PLATFORM



RECOMMENDATION Not to display the permission related to the objective concerned

Technical blocking of the access to the resources even though consent is valid

Can proceed to operations and subsequent processing

RECOMMENDATION not to ask for consent related to the objective concerned in the CMP

No legal basis for the implementation of the distant access and subsequent processing, even though access is technically possible

Can proceed to operations and subsequent processing

This infographic concerns the articulation between the solicitation window (CMP) and technical permissions and not permissions to authorise or refuse the performance of certain actions for a specific purpose.

- Some OS providers provide mechanisms to collect user approval for a specific purpose. Screens presented under these mechanisms can only be a valid means of obtaining consent when they meet the requirements of the GDPR in terms of available information (purposes of processing, identities of actors relying on the given consent) and in terms of the possibility of refusing or withdrawing consent as easily as giving it. Where such screens do not allow valid consent to be obtained, the developer must assist the publisher in analysing the need and, where appropriate, implementing an additional CMP. If a CMP is used to obtain consent for the same purpose, the CNIL points out that it can be considered validly given only if the unequivocal nature of the choice expressed is beyond doubt; this will not be the case if the choice expressed in the permission and that formulated within the CMP differs for the same purpose.
- In any event, a CMP will be required to collect consent for purposes not covered by permission.

6.3. Making good use of SDKs

In practice, when integrating SDKs carrying out processing, the developer chooses the SDKs that he proposes to the publisher, who is responsible for the final decision on integration within the application. The processor developer must not engage a sub-processor without the publisher's specific or general written approval (Article 28.2 GDPR). In addition, in the event that the processor developer integrates an SDK as a sub-processor, it must ensure that that SDK complies with all the controller's data protection requests and must thus reproduce its own obligations within the contract between them (Article 28.4 of the GDPR). It will indeed be responsible in case of failure of this processor. Even if the developer is not a processor, the publisher must be informed and a contract of processing must be directly binding on the application publisher and the processor SDK provider.

1. Select the SDK according to the right criteria

Before any proposal to integrate an SDK, the CNIL recommends that the developer follow an assessment methodology focused on compliance with data protection.

- **What documents should I get from the SDK provider?**
  - The developer must ensure that the SDK only carries out processing that is part of the documented instructions of the controller. The CNIL recommends making sure that the SDK provides documents to determine all the data processing involved in integrating the SDK according to the settings implemented, for example through the record of processing activities.
  - The developer must ensure that the elements enabling the identification of possible unauthorised transfers or disclosures of personal data, within the meaning of Chapter V of the GDPR, are made available (Articles 28.4 and 28.3.a of the GDPR).
- **What analysis should be carried out?**
  - The developer must ensure that the SDK makes it possible to respond to requests for the exercise of rights, in particular the right to withdraw consent (Article 28(3)(e) GDPR). The CNIL recommends giving preference to SDKs providing APIs to respond automatically.
  - It recommends that the developer ensure that the SDK presents ways to block any processing of or access to data stored on the terminal or implementation of a permission until valid consent can be obtained when necessary (see section 6.3.2 'Managing user consent' below).
  - These recommendations also apply to SDKs provided by OS providers or those offered by default in Apple's and Google's documentation for iOS and Android, respectively.
  - As a good practice, the developer can take into account as a criterion the parameter of respect for the privacy of users, for example by choosing solutions that are not financed by monetizing the data of their users.
- **How to integrate a controller SDK?**
  - If the SDK provider implements processing on its own account via the integrated SDK within the application, it is responsible for such processing. This collection must be provided for contractually with the publisher.
  - In some cases, the SDK provider may be a controller and not a processor for certain processing operations carried out on its own account relating to personal data obtained as a processor. In this case, the SDK provider must obtain specific written permission from the original controller for the re-use of the data.[43]
  - In order to allow this process, the CNIL recommends that the developer obtain from the SDK provider the elements to determine its qualification for the processing concerned (see Part 4 of these recommendations concerning the qualification of the SDK provider).

Point of attention

Attention should be paid to the 'Russian dolls' effect: where the integration of one SDK involves the integration of other SDKs, the CNIL recommends ensuring that the initial SDK provides the level of assurance described in this paragraph with regard to its own subprocessors.

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 users' consent when they use tracking devices requiring consent within the meaning of Article 82 of the French Data Protection Act or the carrying out of a processing as a processor based on the legal basis of consent, under Article 28.4 of the GDPR.

- **What safeguards are in place to enable valid user consent to be obtained?**
  - The configuration of the SDK shall allow consent to be given prior to any consent-based processing or reading and/or writing from the SDK. In particular, any reading and/or writing operation within the meaning of Article 82 of the Data Protection Act which requires consent to be carried out on the first launch of the application must be prohibited.
  - The developer must choose SDKs that allow the withdrawal of consent.
  - In cases where the selected SDKs claim that they allow consent to be lawfully collected on behalf of the publisher, the CNIL invites the developer, as a good practice, to contractually note this commitment and audit its compliance (see the proposed method below) in order to enable the publisher to comply with its obligations in this regard.

- **How to ensure the granularity of consent for processing implemented via the SDK?**
  - If multiple purposes are pursued by the SDK, it is recommended that the developer ensure that the SDK supports the granularity of consent, which is generally necessary to ensure that consent is freely given. This means that if consent is obtained for a single purpose, the operations that will be carried out by this SDK will be limited to that single purpose. If several technical operations serve the same purpose, these operations may result from a single consent (e.g. targeted online advertising will usually include advertising selection, control of advertising repetition, audience measurement of advertising, combating advertising fraud, etc.).
  - The CNIL recommends that the developer retain only SDKs that technically allow the suspension of their own executions at an application signal.

3. Auditing the proper functioning of SDKs

The developer may, as a good practice, implement means adapted to the technical complexity of the process, to verify compliance with the commitments of the SDKs it proposes.

- **How to check compliance with the commitments made by the SDK?**
  - A method of auditing by interception of network communications may be considered.
  - The developer may check the effectiveness of the following points:
    - the SDK does not read and/or write (not exempted) before consent is obtained;
    - in the case of consent for different purposes, the SDK respects the choices expressed by the person;
    - the SDK does not collect more data than defined in the record of processing activities provided;
    - the SDK does not access protected resources when authorising access to them for other functionalities;
    - the SDK respects the withdrawal of consent.
  - In case of evolution of the SDK, these analyses can be updated.
  - For the record, the publisher of the SDK, as a processor or sub-processor, has an obligation to facilitate the conduct of such audits.

6.4. Ensure the security of the application

The security of the processing carried out is an obligation incumbent on the developer who processes data on behalf of the publisher (Article 28 GDPR). The developer must, if qualified as a processor, implement all the relevant measures for that purpose and at least all the measures required under Article 32 GDPR.

1. Implement minimum security measures

- **What basic measures are recommended to be implemented in a systematic manner?**
  - Securing communications with servers by systematically encapsulating them in a TLS channel, the cryptographic suites of which are explicitly fixed, in accordance with the ANSSI TLS guide;[44]
  - Storage of cryptographic secrets by packaging using APIs allowing the use of cryptographic suites included in the phone, giving priority to hardware protections such as Android's Hardware *Keystore* or Apple's *Secure Enclave;*
  - Default deactivation of server backups made by third parties (e.g. the OS) or, failing that, encryption of data without including the encryption key in it;
  - Where authentication is necessary, use a means of authentication corresponding to the level of security sought (for example, if a person needs to be authenticated with certainty, do not use a biometric means of authentication if the device used allows the registration of biometric templates of different persons);
  - In general, compliance with the L1 levels of the recommendations produced by OWASP.[45]

2. Adopting an adequate security model

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

- **On what principles is it recommended to base its security model?**
  - Avoid basing its security model on the integrity of the terminal, except in justified cases. For example, in the case of banking applications, it may be justified to seek to certify the integrity of the terminal, to avoid malicious access to passwords. In this case, it is recommended to report the lack of integrity, without causing a blockage.
  - Do not base your security model on certificate *pinning* or code obfuscation measures.
  - Design service in such a way as to maintain the level of security even with corrupt terminals. The recommendations of the CNIL in terms of API[46] are recommended to secure the servers used by the application and protect them against possible attempts at abuse.
  - Protect personal data against possible unauthorised access by processors and implement log-based access controls to prevent internal misuse.

3. Maintaining security over time

- **What measures are recommended to ensure safety over time?**
  - Implementation of deployment processes that ensure the quality of distributed applications is maintained:
    - adopting a continuous integration and continuous deployment ('CI/CD') deployment methodology to enable frequent updates of applications, in particular in the event of a security update;
    - securing code deployment with a prior peer review phase.
  - Maintaining vigilance with regard to external elements integrated into applications:
    - ensuring that the versions used are the most recent;

[44] "Security Recommendations for TLS", ssi.gouv.fr

[45] OWASP *MAS checklist*, mas.owasp.org

[46] 'API [Closed]: the CNIL submits for public consultation a draft technical recommendation',cnil.fr

    - ensuring that there is no malicious evolution in the SDKs implemented, or libraries used via *supply-chain security* practices[47]. To minimise the possible attack surface, using at least elements provided by third parties.
- Keeping the versions available on the application stores up-to-date so as not to endanger users:
    - checking whether it is necessary to impose recent versions of OS, depending on the sensitivity of the data processed, and with regard to the applicable ecodesign benchmarks[48]. And, if this choice is made, leaving available as a remainder (latest version of an application available for a given OS version) only versions presenting a minimal risk in terms of data protection;
    - analysing, depending on the security issues encountered, whether it is necessary to force the update of applications, for example by blocking certain functionality at server level for insecure versions of the application.
- If a personal data breach is established or even suspected, alert the publisher as soon as possible so that it can, if necessary, notify that breach, pursuant to Article 28 of the GDPR.
- Compliance with IT development compliance and security best practices, as outlined in the Development Team's GDPR Guide.

6.5. Checklist

These checks are intended to guide developers in the implementation of these recommendations and are presented as an indication. Some of the checks to be carried out may correspond to good practices or recommendations and not to obligations: in case of doubt, refer to the text of the recommendation.

Category	Subcategory	Identifier	Description
Formalise your relationship with the publisher	Identify the responsibilities and obligations of each	1.1.1	Comprehensive and clear instructions on the processing to be implemented are provided during the contractualization, including the qualification of each of the stakeholders.
		1.1.2	A contact point at the publisher is designated for the validation of any choice affecting the processing of personal data.
		1.1.3	The data is processed only on the basis of the specific instructions provided.
		1.1.4	The obligations of the subcontracting developer (Article 28 GDPR) are identified and implemented.
	Implement project management processes agreed by both parties	1.2.1	Any decision affecting the privacy of users is validated by the publisher in writing, after informing and advising the developer.
		1.2.2	A process for monitoring external developments that may impact processing operations is

[47] 'Attack chain on service providers and consultancy firms: a new threat analysis report',ssi.gouv.fr
[48] General Repository for Ecodesign of Digital Services (RGESN) – 2024, ecoresponsable.numerique.gouv.fr

			implemented, which includes the publisher's alert.
		1.2.3	All the elements necessary for people to be properly informed are sent by the publisher if the publication is delegated to the application stores.
	Identify all processing of personal data	1.3.1	The processing operations implemented by the OS through the use of the functionalities it makes available are identified and validated by the publisher.
		1.3.2	The processing operations implemented following the integration of the SDKs are identified and validated by the publisher. For this purpose, all the information necessary for this classification (list of personal data collected and the purpose, nature and purpose of the processing carried out on these data) is collected from the SDK.
		1.3.3	If certain processing operations carried out in this context contravene the GDPR, the publisher is immediately notified.
Assume its advisory role towards the publisher	Helping to ensure that users' rights are properly respected	2.1.1	The exercise of rights is possible simply, for example by means of a page integrated into the application.
		2.1.2	The exercise of rights includes all processing carried out within the application, including that carried out by third parties such as SDKs.
		2.1.3	A mobile-readable privacy policy is provided by the publisher and integrated into the application in an accessible manner.
	Propose developments respecting the principles of personal data protection	2.2.1	State-of-the-art technical solutions are analysed and proposed to the publisher to minimise collection and limit the impact of making data available to third parties.
		2.2.2	The permissions requested are strictly necessary for the operation of the application. Alternatives to the use of permission are provided for.
		2.2.3	Sensitive data (within the meaning of Article 9 GDPR) is distinguished from other types of data, in particular in terms of architecture.

		2.2.4	Sensitive data is not made accessible to third parties (e.g. SDKs).
	Participate in compliance with the collection of consent	2.3.1	The operations covered by the need for consent are identified and the collection arrangements are validated in advance with the publisher.
		2.3.2	The consents obtained meet the requirements described in the recommendation "Cookies and other tracking devices", adapted to improve readability on mobile terminal.
		2.3.3	If consent and permission are given for the same operation, the relationship between those elements is not such as to create confusion for users or to lead to their being excessively solicited.
Making good use of SDKs	Select the SDK according to the right criteria	3.1.1	Documents making it possible to determine all the processing and data collected during the integration of the SDK is made available by the SDK provider.
		3.1.2	The SDK makes it possible to respond to requests for the exercise of rights.
		3.1.3	Responsibilities are qualified for each of the processing operations implemented as part of the SDK integration, and validated in writing by the publisher.
	Manage user consent	3.2.1	The SDK provides information to ensure the correct information on the purposes pursued when obtaining consent.
		3.2.2	The SDK allows granularity and withdrawal of consent.
		3.2.3	The SDK must allow a configuration that does no reading and/or writing 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 assistance of the SDK provider.
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 physical protections of secrets.

		4.1.3	Backups (including automatic backups) are encrypted with a locally stored key.
		4.1.4	The level L1 of the OWASP MAS is reached.
	Adopting an adequate security model	4.2.1	The security model is not based on the integrity of the terminal.
		4.2.2	Any detection of integrity defects is indicated to the user and not used to block the user.
		4.2.3	APIs integrate elements to secure services.
		4.2.4	Personal data are protected against possible internal misuse or by processors.
	Maintaining 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 the SDKs or libraries used are monitored as part of "supply-chain *security"* practices.
		4.3.3	The application is updated in the event of changes to the OS as a result of security breaches, depending on the sensitivity of the processing operations.
		4.3.4	Any suspected or actual personal data breach is reported to the publisher.

7. Software Development Kit (SDK) Provider Specific Recommendations

How do I read this section?

This section recalls the obligations imposed by the law (e.g. "the controller must") and makes recommendations to comply with them (e.g. "the CNIL recommends"). It is possible for controllers to identify alternative ways of complying with obligations, but they must then be able to justify their choice and engage their responsibility. Some elements are also formulated as good practices and allow to go beyond compliance with the law (e.g. "As good practices, the CNIL encourages").

Notice

To whom are these recommendations addressed?

- Those recommendations are addressed to **suppliers of software development kits (or SDKs), subsequently referred to** as 'SDK suppliers'.
- The SDK provider is defined here as **the entity, natural or legal person, 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.
- The obligations, recommendations and best practices apply to all SDK providers, including when they otherwise assume the role of OS providers or application store.
- These recommendations are specifically addressed within the SDK provider:
  - the Data Protection *Officer (DPO)*of the SDK issuing entity;
  - the technical teams in charge of the development and maintenance of the SDK;
  - teams in charge of commercial relations with partners (developers or publishers), to facilitate integration and manage it contractually.
- These recommendations can also be consulted by other stakeholders in the mobile ecosystem such as application publishers and developers, application 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 the SDK by the mobile applications that integrate it. Such data may be processed by the provider on its own account, on behalf of the publisher of the mobile application, or jointly by both stakeholders. It is imperative that in these different configurations the respective roles and qualification of each stakeholder with regard to the processing of personal data be identified in advance, in particular because an SDK provider can act as both a processor and a controller, within the meaning of the GDPR.
- Nevertheless, there are also SDKs intended to be integrated into mobile applications and offering only local functionalities, or not generating remote processing. As such, their providers act solely as software providers and do not necessarily have a qualification within the meaning of the GDPR, due to the lack of processing of personal data by those providers. 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 that will use it, and to follow the best practices highlighted in these recommendations.

How can these recommendations be used?

- Each section corresponds to a stage in the provision of an SDK by a provider and sets out the privacy challenges and brings together a series of recommendations and best practices to be implemented.
- A **summary list of the main checks to be carried out** is proposed at the end of this section. SDK providers are invited to refer to it, in particular when drafting their contractual documentation, in order to assess the level of consideration of CNIL recommendations by their partners.

See also

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

- Publisher-specific recommendations
- Developer-specific recommendations

7.1. Designing your service

Data protection compliance needs to start at the design stage of SDKs made available to application publishers, where appropriate through their developers (Article 25 GDPR).

1. Identify and analyze obligations with regard to the applicable law on the protection of personal data

The SDK must determine precisely the obligations incumbent on it according to its qualification.

- **What qualifications for the processing implemented by the SDK provider?**
  - As part of the provision of SDK, different qualifications are possible depending on the specificities of the processing of personal data.
  - The SDK provider may refer to Part 4 of these recommendations to characterise all the processing that it is likely to implement in the provision of the SDK. In particular, it is possible to qualify as a processor or joint controller, in the light of the criteria laid down in Guidelines 07/20 of the European Data Protection Board (EDPB)[49].
  - In case the SDK provider is a controller, or co-controller, the SDK provider is invited to consult and also refer to the publisher-specific recommendations.
- **What specific points of attention?**
  - The collection of personal data by the SDK must never be carried out without the knowledge of the data subjects.
  - If the SDK provider is a controller or joint controller, it must pay particular attention to ensuring that data subjects are informed (see Part 4 of these recommendations).
  - The SDK provider, if it is a controller or co-controller, must identify whether the data collected constitutes sensitive data, within the meaning of Article 9 GDPR (see box below).
  - The provider of the SDK as processor must ensure that the controller is aware of the existence of transfers within the meaning of Chapter V of the GDPR[50], in order to provide for an adequate contractual and/or technical framework[51].

For the definition of sensitive data within the meaning of Article 9 GDPR, see Part 5.1 of these recommendations: Ensuring Ensure compliance of personal data processing

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

[50] "Transferring data outside the EU", cnil.fr

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

2. Apply data protection principles by design and by default

The SDK provider shall, for each of the processing operations it implements as controller, analyse whether personal data protection measures by design and by default may apply. The provider must carry out this analysis on all the processing operations carried out by the SDK.

- **How to minimise the data collected?**

  - The principle of minimisation must in particular lead to limiting the data sent to servers (those of the SDK provider, as well as those of its partners) to what is strictly necessary, having regard to the purposes pursued.
  - Default configurations of SDKs that comply with this principle must be proposed, including in the configuration examples proposed in its documentations.
  - In particular, the collection or retention of terminal and network identifiers (IP address, surrounding network hardware) that can be linked to individuals should be avoided if the use of the SDK does not require it.
  - The CNIL invites, as a good practice, the SDK provider to regularly inquire about the existence of more up-to-date functionalities to process certain information (e.g. an approximate location instead of a precise location), which would be more relevant in terms of data minimisation in order, if necessary, to update its SDK.

- **How can the various services be partitioned?**

  - It is recommended that the SDK provider design its service, from the outset, so that its functionalities can be decorrelated from one another and thus allow for a simple configuration of the different options, in particular if the processing of these different options entails different responsibilities.
  - For example, if the SDK provider provides audience qualification services (as a processor) but also data collection for retargeting purposes on its own behalf (as a controller), the independent selection of these two functionalities by the publisher could be allowed for SDK integration, possibly with a paid alternative if this choice impacts the business model of the SDK provider. If these functionalities require the user's consent, this technical decorrelation is necessary.
  - In the same vein, the CNIL recommends that the SDK provider avoid, as far as possible, grouping all the services and functionalities offered within a single 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 processing?**
  - 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 functionality sought. For example, a conversational assistant module may wish to have voice input, which requires microphone access permissions, but does not need to require acceptance of that permission in order to work.
  - The CNIL recommends that the provider ensure that it chooses the least intrusive level of permission possible, or that it offers different configurations to the user's choice.
  - The SDK provider must also distinguish between permissions relating to the service rendered to the application and subsequent permissions and data processing that it carries out on its own behalf and which are sometimes linked to its business model.
  - It is recommended that the SDK be as little dependent as possible on obtaining permissions, in particular by studying the use of alternatives as presented in section 5.5 of these recommendations ('Permissions and data protection by design'), whether those alternatives are in the hands of the direct users (publishers or developers) or the user of the application.

7.2. Documenting the right information

The SDK provider must provide its partners (publisher, developer) with the necessary documentation so that they can ensure their compliance. When acting as a controller, it must also document its compliance.

1. Identify the information to be provided

- **What information should be documented on the processing implemented?**

- The CNIL recommends that the SDK provider draw up and make available to its customers an analysis of the processing operations involved in the use of the SDK, whether the provider merely provides the software or plays an operational role in the practical implementation of the processing operations. The provision of this information will enable the publisher to respond precisely to the requirements of the application stores, which are prerequisites for the publication of a new application or its update on the store.
- Where processing by the SDK provider is likely to result in a high risk to the rights and freedoms of individuals, the SDK provider has an obligation to draft a DPIA (see Article 35 GDPR).
- For each processing, it must identify its qualification within the meaning of the GDPR.
  - The CNIL recommends that this qualification be defined in conjunction with its partners.
  - According to that classification, when acting as a controller, the SDK provider must keep and maintain its own record of processing activities, in accordance with Article 30 of the GDPR;
- If it acts as a processor and processing involves the use of a third-party sub-processor, it must obtain authorisation from the controller and ensure that the same data protection obligations under the contract with the controller are imposed on that sub-processor, by contract or any other legal act (Article28 GDPR).

What information should be documented on the use of tracking devices?

- The SDK provider must accurately inform its partners, either the controller if the provider acts as a processor, or any other joint controllers, of read and/or write operations on the user's terminal (this can be done by referring to the developer-specific recommendations for the identification of such occurrences).
- It must indicate the purposes pursued by each of these uses of tracking devices. If it is neither a controller nor a processor, the CNIL invites, as a good practice, the SDK provider to document the functionalities including tracking devices, to enable the various stakeholders to meet their possible obligations.

What information to document about permissions?

- The SDK provider must inform its partners, either the controller if the provider acts as processor, or any other joint controllers, 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 of Article 82 of the French Data Protection Act, which may require specific consent from the user.
- It is recommended that it specifies the optional or mandatory nature of these operations according to the proposed functionalities.

2. Present this information in an accessible format

This information can ideally be made available in an accessible format and a formalism facilitating their analysis, regardless of the settings relating to the processing implemented.

How are they to be made 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 any consents, must be formalised in the contractual documentation.
- The CNIL recommends that any evolution of the service impacting privacy issues be made available to the partners of the SDK provider and be expressly indicated to them. If the SDK provider is a processor, these developments must also be approved by the controller before they are implemented.

What formalism should be adopted?

- Article 30 of the GDPR makes it mandatory for controllers (see paragraph 1) or processors (see paragraph 2) with more than 250 employees (see paragraph 5) to keep a record of processing activities, which must include, in particular:
    - This record must separate each of the processing operations carried out, a processing operation being defined by its purpose. If processing depends on the chosen parameters, it is recommended to provide partners with a dynamic record according to the settings of the SDK. Otherwise, the parameters related to each processing should be indicated so that partners can understand which processing are implemented as part of their particular configuration.
    - For each processing, the data collected must be explicitly indicated. To facilitate reading and analysis, it is recommended to choose a format that allows easy manipulation of the information, for example via a spreadsheet file (thus making it easy to identify all processing operations relating to a given data).
    - For each processing operation, it is mandatory to also indicate the legal basis identified and the obligations deriving from it.
    - The CNIL suggests as a good practice that the record of processing activities should be designed in such a way as to be able to extract useful information from it for the partners of the SDK provider, identifying in particular what is a matter of business secrecy.
- As a good practice, where the SDK provider is responsible or jointly responsible for the processing of these operations, it is encouraged to document the storage or gaining of access to information stored in the terminal it implements. For example, he may present this information in an legible table:
    - indicating, for each line, the operation carried out, the associated permission, the purposes pursued (and potentially the corresponding record item) and the technical means to block or activate this reading (in order 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 versions of the SDK that use each line, to allow partners to choose the appropriate version and understand the effects of a possible update of the SDK that they have integrated.

7.3. Managing consent and people's rights

As a processor, the SDK provider can have a strong impact on the respect of the rights of individuals, in particular by facilitating the exercise of rights and by designing means to facilitate the collection of consent.

1. Assisting in the proper exercise of users' rights

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

- **How can data subjects be informed about the processing of personal data relating to the SDK?**
  - If the SDK provider is a controller or joint controller, it has an obligation to ensure that individuals are informed. It is recommended that this information is directly integrated into the information provided by the publisher to the user.
  - In particular, the transmission of personal data of users to business partners, for example for the purposes of monetising the application, must be explicitly brought to the attention of individuals. If the processing operations in question require consent, the information given must be such as to enable the data subjects to assess the consequences of their choice by informing them of the extent of that choice. The CNIL recommends to draw the attention of the data subjects to the number and the sector of activity of the partners who would be made recipients of the data.
  - The CNIL recommends that the SDK provider include in its contract with the publisher or developer the obligation for them to provide information on its processing operations.
  - The same applies to the information that must accompany a request for consent for the processing operations for which the SDK provider is responsible.
  - Where applicable, the SDK provider may offer an interface software component (like a CMP) that can also be integrated into the application and that allows the collection of user consent for those purposes =.
  - It is recommended that the SDK provider monitors developments in the data privacy policies of the partners, to ensure that the processing mentioned therein correspond to the processing actually implemented. If it is a processor and finds that information is missing or too general, the CNIL recommends reporting it to the controller, pursuant to Article 28(3) of the GDPR.

- **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. The SDK provider, if it is a processor, has an obligation vis-à-vis the controller to facilitate compliance, the content of which depends on the functions contractually entrusted to it. The exercise of rights may also concern processing under the own responsibility of the SDK provider, who must then be fully responsible for ensuring compliance with the rights available to individuals under the GDPR.
  - The exercise of rights must be considered from the outset, particularly in terms of the structuring of databases. The right of deletion, in particular, must be able to be respected independently of technical constraints.
  - In particular, in the event of the transmission of personal data of users to business partners, for example for the purposes of monetising the application, the SDK provider must pay particular attention to making it possible to exercise the applicable rights.
  - To facilitate the practical implementation of the exercise of rights, the CNIL recommends that the possibility of automating it 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 is invited to use as few additional identifiers as possible to process the exercise of these rights. For example, if data is associated with the person simply on the basis of an advertising identifier, this could be sufficient to enable the exercise of human rights. Conversely, in the light of Article 11 of the GDPR, it is possible that a request for the exercise of rights may not receive an effective response. For example, in the event that the person resets their advertising ID and is no longer aware of the previous identifier(s), additional information gathering may be necessary to identify the person.

2. Participate in compliance regarding the use of tracking devices and the collection of consent

If the qualification of the SDK provider is that of a processor within the meaning of the GDPR, the CNIL recommends that the latter provide the controller with practical advice, in particular on the possible need to obtain consent, to provide the technical means to allow 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 French Data Protection Act or under the GDPR are recalled in part 5.1 of these recommendations: "Ensuring legal compliance of processing operations".

- **Can the permissions granted by the user to the application be used to obtain consent to the processing carried out by the SDK?**
  - Where access to a terminal resource by the SDK requires the consent of the user, it is imperative that the controller ensures that valid consent has been obtained for each purpose pursued.
  - If access by the SDK to a terminal resource and the resulting processing requires the user's consent, the user cannot be considered to have been obtained solely on the basis of permission granted to the application. In particular, if permission is granted to the application for a purpose other than that of the SDK, that permission cannot be regarded as valid consent of the data subject.

- **How to allow a valid collection of consent?**
  - The CNIL recommends that technical and organisational means, allowing the blocking of any processing or access to data stored on the terminal (or system permissions allowing it) be offered, until valid consent is obtained. It is therefore recommended that the provider provide for its SDK to be able to suspend its execution until consent has been obtained.
  - For consent to be valid, it must be given in a specific way (in particular as distinct from the acceptance of the conditions of use of the application) and free (which implies in principle being able to choose whether to grant or refuse consent depending on the different types of purpose).
  - As such, if the processing serves several distinct purposes, the signals relating to the user's consent must be taken into account in their granularity, purpose by purpose, regardless of the status of the permissions requested.
  - For each of the consents sought, it is recommended that the design and documentation of the SDK provide for the possibility and anticipate the functional impacts of a lack of user consent, in order to minimise any unnecessary blocking of functionalities in case of refusal.
  - The revocation of consent for these purposes must properly be taken into account after it has been initially granted. As such, the CNIL recommends that the SDK provider 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 is invited to ensure that the use of *'install-time permissions'* is limited as much as possible*,* preferring the use of '*runtime permissions*', in order to facilitate possible integration with the application publisher's collection tools and, where justified, in such a way as to contextualise consent requests. Thus, if the functionality in question is never used, the relative permission should not be displayed. The CNIL points out that, in certain cases, the establishment of a block of permission during the installation, permission that might not be used, is likely to be contrary to the obligation to configure data processing in the most protective sense of privacy (privacy by design*,* Article 25 of the GDPR).

7.4. Participate in maintaining compliance of the application over time

The SDK provider, when qualified as a processor, must 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 stakeholders providing executables, such as the external developer of an application. In cases where the SDK provider is a simple software provider, it is encouraged to follow these recommendations as a good practice.

- **What security measures should be implemented?**
  - See recommendations in section 6.4 of these recommendations: 'Ensuring 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 processor, the contract or legal act governing the subcontracting must include an obligation on the provider to allow audits to be carried out (Article 28(3)(h) of the GDPR).

- **How can audits be facilitated?**
  - To facilitate such audits, the processor SDK must make all information necessary to demonstrate compliance with its obligations under Article 28 GDPR (as well as that of any processor) available to its customer, including up-to-date technical documentation (see above).
  - The SDK provider is recommended to have audits carried out on its SDK on a regular basis and on its own initiative in order to anticipate and prevent problems that could subsequently be identified by its partners, joint controllers or controllers, or by the supervisory authorities.
  - As a good practice, it is recommended that SDKs offer a deactivation feature that can be easily activated by the publisher, remotely and in production, in the event that, following an audit, legal uncertainty, malfunction or any other event, the publisher wishes to pause only the processing of the SDK for the time required to resolve the problem, without having to render its entire application inoperative.

3. Implement robust processes in terms of compliance

The SDK's continued compliance should last over time, with processes in place to update it as implementation conditions change.

- **What measures should be put in place to ensure safety over time?**
  - The CNIL recommends that tools and methodologies for reporting vulnerabilities, in the event of proven exploitation, be put in place. As a processor, the SDK provider is required to inform its controller in such a way as to enable it to comply with its obligations regarding the security of personal data (Articles 32 to 36 GDPR).
  - In the event of a personal data breach within the meaning of the definition in Article 4 GDPR , the SDK provider that is controller or joint controller for the processing concerned must itself notify the data breach to the authority of the country to which the entity belongs or ensure that (Articles 33 and 34 GDPR) or ensure that such notification was made by its joint controller, where applicable.
- **How to take into account the possible evolutions of its partners?**
  - The SDK provider is also invited to monitor the technical developments of the APIs offered by the operating systems. Indeed, OS updates often lead to changes in the functioning of certain methods, which can have privacy impacts. The CNIL considers it a good practice for the provider to update its SDK in line with technical developments in the OS, in particular by studying whether these developments can make it possible to implement the processing operations in a more privacy-friendly manner. If this is the case, it is invited to update and encourage the use of the most recent versions of its tool.

7.5. Checklist

These audits are intended to guide SDK providers in the implementation of these recommendations and are presented as an indication. Some of the checks to be carried out may correspond to good practices or recommendations and not to obligations: in case of doubt, refer to the text of the recommendation.

Category	Subcategory	Identifier	Description
Designing your service	Identify and analyze its obligations with regard to 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.
	Apply data protection principles by design and by default	1.2.1	The data collected by the SDK as well as those transmitted to partners are minimized.
		1.2.2	The various functionalities offered by the SDK can be integrated and executed in a decorrelated manner, in particular if they do not all involve the same responsibilities or purposes.
		1.2.3	Rather than grouping several different functionalities within a single SDK, they are split into several separate SDKs.
		1.2.4	The permissions required to run the SDK are minimised, distinguishing between those that are strictly necessary and those that are desired but not essential.
		1.2.5	Where more than one permission can allow data to be collected in its desired form, those with the least intrusive technical capabilities is chosen.
Documenting the right information	Identify the information to be collected	2.1.1	A clear analysis of the processing operations entailed by the use of the SDK is carried out and accessible.
		2.1.2	For each processing, the qualification of the stakeholders, within the meaning of the GDPR, is identified.
		2.1.3	For each processing operation involving the use of a processor, the purpose analysis is carried out and the authorisation of the controller is obtained.
		2.1.4	The presence of tracking devices implementing reading or writing on the end-user's terminal is indicated precisely and explicitly, explaining the purposes pursued.
		2.1.5	The optional or mandatory character for each of the permissions required by the SDK is indicated, depending on the features used.
		2.2.1	The above documentation and information are up-to-date.

	Present this information in an accessible format	2.2.2	The above information is formalised in the contractual documentation where it needs to be formalised.
		2.2.3	Specific information is provided when updates to the SDK involve an evolution of the processing implemented.
		2.2.4	The record of processing activitiesclearly distinguishes the purposes associated with each processing operation.
		2.2.5	If the intended purposes depend on the configuration of the SDK, a dynamic or separate record is made available, depending on the configuration possibilities of the SDK, so that the controller can easily identify the elements of the record that correspond to its configuration.
		2.2.6	The format of the record, for example in the form of a table, makes it possible to easily and exhaustively identify each data collected, as well as the associated legal (legal basis, purpose, obligations) and technical (readings, records) elements.
		2.2.7	Examples of wording relating to the processing carried out are directly proposed, so that a third-party partner can easily reuse them for its own collections of consents.
Managing consent and people's rights	Assisting 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 such requests can be automatically reflected in the technical infrastructure of the SDK.
		3.1.2	The establishment of these APIs does not use, or as little as possible, additional identifiers, so that these requests for rights can be effectively answered.
	Participate in compliance in terms of use of tracking devices and collection of consent	3.2.1	The mere obtaining of permission cannot be considered as indicating that consent has been validly obtained for the processing carried out by the SDK
		3.2.2	The SDK is technically designed to allow its execution to be suspended until valid consent, by purpose, is obtained.
		3.2.3	If several purposes are pursued, the SDK technically allows a separate signal per purpose to be taken into account, always independently of system permissions.
		3.2.4	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.
		3.2.5	The revocation of consent does not affect the proper execution of the third party partner’s application, both functionally and vis-à-vis the user experience (such as a consent request displayed in a loop).

		3.2.6	Requests for system permissions are made during the execution of the application rather than during its installation, where possible.
Participate in maintaining compliance over time	Offer secure SDKs	4.1.1	Refer to sections 4.1.1-4.3.4 of the Developer Checklist.
	Allow audits to be carried out	4.2.1	Audit reports of the SDK are carried out on a regular basis and are made available to partner publishers and data protection authorities upon request.
		4.2.2	The SDK may be paused by the publisher, remotely and in production, in the event that the result of an audit would lead to legal uncertainty or technical malfunction.
	Implement robust processes in terms of compliance	4.3.1	A technical and organisational process for possible data breaches is established, which provides for the transmission of information to controllers as well as the formalism of breach notifications to data protection authorities.
		4.3.2	Regular monitoring is applied on technical developments of mobile operating systems and the APIs they make available, in order to reinforce the principles of protection by design and protection by default.

8. Operating System (OS) Provider Specific Recommendations

How do I read this section?

This section includes elements that are formulated as good practices and allow to go beyond compliance with the law (e.g. "As good practices, the CNIL encourages"). It also recalls the obligations imposed by the regulations (for example, 'the controller must') and makes recommendations to comply with them (for example, 'the CNIL recommends'). It is possible for controllers to identify alternative ways of complying with obligations, but they must then be able to justify their choice and engage their responsibility. Some elements are also formulated as good practices and allow to go beyond compliance with the law (e.g. "As good practices, the CNIL encourages").

Notice

To whom are these recommendations addressed?

- These recommendations are addressed to **operating system (OS) providers** designated as 'OS providers'.
- The OS provider is defined as **the entity that makes an operating system available on a terminal.**
- Depending on the situation, the operating system may be:
  - developed in its entirety by an entity for exclusive use on terminals it makes available (e.g. iOS, developed by Apple);
  - developed in its entirety by an entity for licensed use on terminals produced by third parties (e.g. Android, developed by Google);
  - based on a pre-existing OS whose license allows reuse, which is then modified by an entity (through a plug-in process, or "fork"), for use on its own terminals or for making available to end-users of the terminals (e.g. LineageOS, based on Android Open Source Project and developed by LineageOS LLC).
- These recommendations are not intended to cover the obligations that apply to the OS provider, apprehended as an application publisher, or as an SDK provider. **The OS provider also publisher of the system applications (whether or not pre-installed on the user's terminal) or SDK provider shall be subject to the same qualifications and obligations as any application publisher or SDK provider,** respectively. To this end, it refers to the recommendations applicable to these stakeholders.
- These recommendations are addressed more specifically within the OS publisher:
  - the Data Protection *Officer (DPO);*
  - the developers and lawyers of the entities that provide these OSes.
- These recommendations can also be consulted by other stakeholders in the mobile ecosystem: application publishers and developers, providers of application stores, software development kits (SDKs), etc.

What is the purpose of these recommendations?

- OS providers are often required to process personal data as part of the normal operation of the terminal and the applications run by the user. As such, the functionality of the APIs they make available to applications plays a major role in the ability of application publishers to offer content that complies with applicable data protection rules. **The CNIL encourages OS providers to enable configurations that facilitate compliance of applications.**
- Moreover, in the context of the publication of an OS under a licence allowing its reuse and whose source code is accessible, design choices are likely to be passed on, identically or in a similar form, by all stakeholders reusing the published source code. As a good practice, 'privacy by design' measures can be

implemented by OS providers so that all stakeholders in the chain reusing the code can benefit from them and, ultimately, improve the protection of the privacy of the end users of those OS.

- Some providers choose to integrate a set of third-party applications into their OS. These technological choices involve numerous data processing operations which they must identify, both in terms of the consequences for individuals and the resulting legal qualifications within the meaning of the GDPR.

How can these recommendations be used?

- Each section corresponds to a step in the provision of an OS by a manufacturer itself, to other manufacturers or directly to end-users and sets out the privacy challenges and brings together a series of recommendations, as well as best practices to be implemented.
- These recommendations are without prejudice to rules applicable on other legal grounds than the protection of personal data, in particular competition law.
- A **summary list of the main checks to be carried out** is proposed at the end of this section. OS providers are invited to refer to them, in particular when drafting their contractual documentation.

8.1. Ensure the compliance of the processing of personal data implemented

Although the role of the OS is to provide functionalities for the use of application developers, it is possible that some processing of personal data is carried out on its own. As such, the OS provider must comply with the obligations regarding such processing.

1. Determine the share of the OS provider in 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.

- **Which entities can participate in the implementation of personal data processing in an OS?**
    - As the OS is not necessarily provided in its entirety by a single entity, each provider must conduct an analysis of its responsibilities, which will depend on the actual supply of functional bricks and processing used by applications and people.
    - That analysis must be carried out where the OS provider determines *'the purposes and means of the processing'* (Article4.7 of the GDPR),and is therefore responsible for the processing carried out by an item made available by it.
    - 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 section 2 of these recommendations 'Who are the stakeholders operating in the mobile applications sector?'):
        - if it is an entity developing and making available an OS intended to be run (only or mainly) on its own terminals;
        - if it is an entity reusing third-party software bricks on its own account, in order to offer a new OS, for example for use on its own terminals;
        - in the case of an entity developing and making available an OS intended to be executed on third-party terminals, where that execution implements processing operations on its own account.
- **Which processing of personal data may be affected?**
    - The question of the processing operations that may carry the responsibility of the OS provider is detailed in Part 4 of these recommendations, in particular 'Qualification of the OS provider'. When the OS is limited to providing software tools whose processing is confined to the terminal, it is a priori neither controller nor processor within the meaning of the GDPR.
    - The processing operations concerned may be linked to functions implemented in different contexts, for example:
        - data processing relating to the use of sensors (e.g. pre-processing of location data);

    - data processing relating to the provision of functionalities to applications (e.g. notification services, management of unexpected terminations, so-called "crash", and remote backups);
    - OS-specific data processing (e.g. telemetry and bug reporting).

2. Apply data protection principles by design and by default

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

- **Is the default setting of the OS as intrusive as 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 operation on the terminal not exempted from consent occurs before the collection of a valid consent under the GDPR and the Data Protection Act.
  - He must ensure that this consent is collected specifically and separately 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 consent for those purposes.
  - It is recommended that the OS provider allows the user to use their terminal, including default applications or those installed on their own, without the need for account creation. It is recommended to avoid *'dark patterns'* intended to encourage them to create an account to use their terminal if this is not necessary.[52]
- **How can the data processed by the OS as controller be minimised?**
  - As regards the transmission of notifications to users of the application, the OS provider is invited, as a good practice:
    - allow the use of third-party notification servers, optimising their use so as to minimise the impact on the terminal's capacities, for example in terms of battery capacity;
    - to offer developers, in order to improve the confidentiality of user data, up-to-date tools enabling the encryption of the data contained in notifications, regardless of the system in charge of transmitting them. As such, it can clearly indicate how these tools are used in the documentation for developers.
  - Regarding telemetry and bug reporting:
    - the OS provider is invited to propose a bug report 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 processors have access to bug and crash data;
    - it is recommended to allow publishers and third parties to obtain consent (where necessary) from users prior to each retrieval of such data or their transmission to third parties.
  - With regard to remote storage of backups:
    - it must ensure that they are carried out only following an explicit request from the application and not by default;
    - it is asked to allow encryption of these, preferably by default, with a key that is not accessible to the OS provider itself.
  - With regard to the pre-processing of location data:
    - the OS provider is invited to allow the application making use of location data, as well as the user, to easily limit the use of location to GPS sensor data only, without the need to use other services and sensors such as the surrounding Wi-Fi or Bluetooth connections.
    - for the location service based on surrounding connections, a method of calculating the precise location on the terminal and not on the server must be preferred: by way of example and best practice, the terminal can transmit the list of surrounding connections to a responding server by providing it with all connection information in a

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

wider perimeter, after which the terminal locally performs the calculation of the precise location on the basis of this precise information.

- the OS provider is encouraged to offer the possibility for the user to be able to easily set up a suspension of the constant location collection, for the OS itself or for third parties, so that it is active again only when it is necessary for a user's use of an application. Thus, a user could be offered the possibility that his location is not collected except when his uses so require, without having to manually activate it beforehand in the settings of the OS, and then have to return to disable it after each use.

8.2. Ensuring that partners are properly informed

Due to their expertise in the processing they carry out and the functionalities they offer, OS providers are best placed to provide documentation and advice for the proper use of the proposed functionalities. As a good practice, a set of measures can be implemented to this end.

1. Provide comprehensive documentation to support publisher and developer compliance

In order to facilitate the proper understanding of the functionalities of the OS, its provider is invited to make available comprehensive technical documentation, allowing its publisher and developer partners to analyse and legally qualify their responsibilities within the meaning of the GDPR. As a good practice, a general reminder of the legislation to be taken into account could be made available by OS providers. However, this provision must not impose specific compliance procedures on the partners.

- **To whom should this documentation be addressed?**
  - While it is common for technical documentation to be made available, the CNIL suggests including elements recalling the specific legislative and normative framework of the European Union, for publishers and developers who wish to target the European market;
  - These legal elements could thus be grouped together with the technical elements in order to enable informed decision-making on their consequences;
  - The CNIL suggests that these elements, and in particular the legal content, be made available in a language understood by the target public.

- **What elements should be included in this documentation?**
  - For publishers targeting the European market, the CNIL invites the OS provider to alert in particular to the need to define their responsibility and to put in place compliance measures (purpose, information, rights, security, etc.);
  - In addition to the technical elements, it is suggested to include specific guides and tools for DPOs so that they can integrate them directly into their risk analysis and continuous improvement methodologies.
  - In the event that the OS makes available several functionalities that can serve the same purpose (e.g. different location APIs), the CNIL invites the OS provider to specify their technical and legal characteristics to allow the publisher and the developer to make an informed choice. In particular, the criteria of backward compatibility, end of support, vulnerability, energy optimisation, shift of the calculation logic, transfers, etc. could be presented.
  - It is recommended to indicate in the official documentation whether or not the tools made available meet legal obligations such as the collection of consent respecting the criteria of the GDPR (see section 8.3 'Providing tools to enable the respect of users' rights and consent'), and if so with what configuration.

2. Inform third parties of the processing operations specific to the OS

With regard to 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, where the use of functionality made available by the OS to applications entails the implementation of processing by the OS.

- **What information should be made available?**

- The CNIL recommends that the OS provider ensure that its partners (third-party developers and publishers, application stores, manufacturers, 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 this context, it will be necessary to indicate, for the functions activated by them:
  - the data processed exhaustively for the chosen configuration;
  - the legal qualification, in particular as regards 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.[53]

- **On which functions should third parties be informed?**

The CNIL recommends that OS providers:

- provide detailed information on the function identified in the previous section (backups, notification, telemetry);
- 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 of the GDPR (see box below);
- explain the impact of the default settings and functions of these devices.

For the definition of sensitive data within the meaning of Article 9 GDPR, see Part 5.1 of these recommendations: Ensuring compliance with the processing of personal data

3. Encourage the use of the most privacy-protecting features

The CNIL encourages the OS provider to make available details of the characteristics of the various functionalities it offers. This good practice should allow publishers to make an informed decision about their use, in order to meet the requirements of the laws on the protection of personal data.

Thus, where the OS provider offers a more privacy-protective functionality to process certain information (e.g. a rough location instead of a precise location), which seems more relevant in terms of data minimisation, the CNIL suggests that it informs SDK publishers, developers and providers of its existence, as well as the possibility to update their code to benefit from it.

- **What are the best practices to encourage the adoption of the most privacy-friendly technologies?**

- The OS provider may further inform application publishers and developers, over time, about their use of the new APIs offered by the OS:
  - listing the various changes made and presenting practical cases;
  - specifying in a detailed and justified manner the legal consequences for its partners (effects in terms of compliance, consequences on the publisher's obligations, etc.);
  - indicating, where appropriate, in a detailed and justified manner, the implementations that comply with the principles of data protection by design and by default (Article 25 GDPR).
- The OS provider may compile statistics on the prevalence of the use of the most advanced functionalities, and use this information to selectively communicate on the ignored functionalities.
- It can organize the gradual end of support for the most intrusive and permissive features in terms of possible data collection, with a sufficient transition period to allow publishers to update their applications.
- Finally, it could 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.

[53] "Transferring data outside the EU", cnil.fr

8.3. Provide tools to enable respect for users' rights and consent

The functionalities made available by the OS provider to the publishers and developers of applications may have an impact on the compliance of the processing operations implemented by publishers and developers. The CNIL encourages the OS provider, as a best practice, to take utmost account of this when designing these functionalities.

1. Permission systems that respect the principle of data protection by design

The permission system provided by the OS is at the heart of user protection : by allowing access to certain data to be technically blocked depending on the user's choice, permissions provide a technical guarantee that applications respect the confidentiality of information and are a direct means for individuals to preserve their privacy

Only technical permissions intended to grant or block access to certain protected resources are considered here, irrespective of the purposes for which access to those resources is requested. Permissions to authorise or refuse the performance of certain actions for a specific purpose (such as the collection of an advertising identifier), through access to certain resources but also by other means, are excluded.

Permissions must in any case be designed in accordance with the rules of competition law. In particular, they must not lead to favouring applications that the OS provider has designed or pre-installed. Thus, permissions designed by the OS provider must be presented in the same way as for any other application. Moreover, permissions should not be designed to prevent publishers from accessing relevant data but to ensure that people can have control over their data, in compliance with DMA and competition law.

- **What operations should permissions be applied to?**

The CNIL considers it good practice that the OS provider:

- apply access permissions to the user terminal, whether to its sensors (camera, GPS, environmental sensors), its functionalities (network access, Bluetooth, NFC), or its storage (contacts, photo gallery, mass storage);
- requires the information and collection of the user's permission for all of these elements, preferring systematic use of permissions that are visible to the user;
- provides for the collection of a permission from the terminal user regardless of the legal obligation to collect or not a consent under Article 82 of French Data Protection Law for the operation of reading information stored on the terminal.

- **What scope to choose for permissions?**

- When a permission is defined, its scope can be analysed under three distinct axes:
  - the degree of accuracy of the data provided: 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, access permissions to physical sensors (e.g.: barometer, thermometer, photometer, gyroscopes, accelerometer) may sometimes suggest a limitation of their accuracy; note that the level of accuracy of the data should also be clearly indicated to the stakeholder using the data (application publishers and their processors);
  - its material scope: each permission may apply to a larger or smaller set of data or functions. Permissions that are too broad in terms of material scope are likely to result in over-collection by applications (which may, in some cases, be contrary to the principle of minimisation). A good practice would be, for example, to avoid global permissions to access stored files, favouring an access system per file or folder;
  - 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 may be left

to the user, possibly accompanied by suggestions of values from the publisher of the application. This temporal scope can also take into account contextual elements, such as whether the application is active or not, in the foreground or not, or on the contrary inactive for a fixed period of time.

- The CNIL invites the OS provider to offer the finest possible degree of control to the user to restrict the scope of each permission according to these three axes.

- **What additional measures?**

As a good practice, the CNIL invites the OS provider to:

- systematically provide that permission may not be required before the launch of the application but only when the application needs it;
- encourage, in documentation and best practices shared with developers, the collection of permissions in a contextual manner, when they are needed;
- give users the possibility to choose the level of information they wish to transmit under this permission. For example, the user could have the possibility, in case of a request for access to his contacts, to return a partial list of them. In this case, the OS provider must ensure that the information transmitted to the application is transmitted in the same technical format regardless of the choice of the user, so as not to affect the technical functioning of the applications. This parameterisation option left to the user must be implemented by the OS provider under transparent, fair and non-discriminatory conditions.
- allow users to allow access only once or only when the application is active, in the foreground or used, in particular for the most intrusive permissions, i.e. those posing the greatest risk to the privacy of individuals, in particular because of the possibility of activating them occasionally without the user's knowledge or continuously (e.g. location, camera sensor, microphone). If the application requires permission 'at any time' (including when the application is closed), the information when obtaining the user's consent may be strengthened;
- periodically revoke the permanent permissions of unused applications, notifying the user of such revocation, so as to allow the user to set the frequency of such reminders (e.g. one month, six months, one year) or to disable them if he or she so wishes;
- establish isolation between the execution of the application itself and the execution of the 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 provided to the user.

2. Helping to ensure proper compliance with users' information and consent obligations

By providing tools for this purpose, the OS provider is able to simplify the implementation of the respect of users' rights and consent.

- **How can the right information be provided to users?**

Permission systems, which are usually a step to trigger the processing of personal data (location, contacts, etc.), need to technically allow the publisher to provide the relevant information to the user on the scope of the permission it gives (see section 5.5 of these recommendations, 'Permissions and data protection by design').

As a best practice, the CNIL invites the following design elements to be taken into account:

- Beyond mere prior information, it is desirable that the user continues to be informed during and after the processing. As such, transparency measures on access to sensors, in particular via visual indicators on punctual accesses, at the time they are carried out by the system, but also at the time they are carried out by an application, specifying then which, can be implemented.
- The user can have access to a history of sensor activation and queries made, filtered by usage and by system process or application. In addition, an indicator can be displayed, for example in the status bar, indicating when permission is used.
- For the most intrusive permissions (access to the microphone, camera, location, files on the phone, contacts, calendar), it may be planned to repeat the permission request some time after

the first permission, so that the user can reverse their initial choice at the time they first implemented the application. This would make it easier for users to reconsider their choice of permissions, including for applications pre-installed by the OS provider. Setting up such a setting presupposes that it is possible for the user to set the frequency or activation of these reminders, for example during the initial configuration of the OS when using the mobile device for the first time.

- **How can we help with the proper collection of consent?**

  - It is common for requests for permission 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 compliance of applications while minimising user fatigue, permission windows may, in certain limited cases, allow valid consent to be obtained directly. Such cases include, for example, permissions which correspond to a single processing operation, a single purpose and a single recipient of the data. To this end, these windows must contain:
    - the sole purpose for which permission is sought;
    - hyperlinks to access all the information provided for by the legislation (Articles 13 and 14 of the GDPR, Article 82 of the French Data Protection Act);
    - the modalities for revoking access.
  - In this case, it is up to the developer to ensure a good articulation between permission and the collection of consent (see table in section 6.2.3 of this recommendations).
  - The CNIL recommends that the publisher be given some latitude in terms of the information presented to the user at the time of the request for permission, in order to ensure sufficient information for individuals (see section 5.5 of these recommendations, 'Permissions and data protection by design').
  - As a matter of good practice and depending on the intrusive nature of the permissions, the OS provider can ensure that the user has sufficient information on the impact of his choices. A link to understand this impact could be made available, setting out a series of concrete examples and associated risks. For example, for a permission to access the SMS of the terminal, it can be specified that it can legitimately be a question of recovering a temporary password as part of a multi-factor authentication, but also the capacity for a malicious application to read, transmit or modify the received SMS in time. Such information would be such as to enable the user to estimate the interest in authorising such collection on the basis of the degree of trust he has in the publisher of an application.
  - Finally, it can make it easy to revoke or change permissions granted by the user.

- **How can data portability be facilitated?**

  - Even in cases where it does not endorse a classification as a controller, the CNIL considers it a good practice that the OS provider allows the portability of personal data to be implemented, by means of an open format. This portability, which becomes an obligation for the OS provider if it is the controller, may in this respect concern the configurations but also the applications installed on the phone, so as to promote dialogue and cooperation with the providers of other OS. As a good practice, it may consider Articles 4-1 and 20 of the GDPR, which call for the definition of a 'structured, *commonly used and machine-readable format',* so that it is relevant for a user wishing to carry his data from one OS to another.

3. Protecting Minor Users

The processing of data of minor users by application publishers is subject to specific obligations. The OS can provide useful tools for their implementation as a good practice.

- **How to participate in the compliance of applications with regard to minor users, within the meaning of Article 8 GDPR?**

- The CNIL invites OS providers to provide parental control tools that include, via an API or other non-intrusive technological modalities, the possibility of notifying applications of the relevant age range of the person, depending on the parameters that may have been previously filled in the OS, in particular by the child's parent or legal guardian.
- The parental control tool could thus be used directly on the terminal without having to provide additional information to a third party (such as the OS provider itself or the publisher of a third-party parental control system), or requiring the creation of a user account on an online service solely for that reason.
- Such a solution would help application developers to define whether the user is a minor, in order to facilitate compliance with the obligations under the GDPR and minimising the need for remote processing.
- The fact that a given user is a minor could be taken into account directly in these tools, inducing their ability to respond to possible system permissions via effective parental control tools.
- The possibility of registering several profiles within biometric authentication vectors would make it possible to distinguish whether the authenticated user is the minor or his or her legal representative, so that it would be possible for developers to configure an application where the minor's permission is sufficient for certain actions, and where the legal representative's permission is necessary for other actions.

8.4. Provide a secure platform

The OS is the basis for the security of the terminal. As such, OS providers are invited to ensure that they make available state-of-the-art elements to provide this security guarantee to users.

1. Ensure the security and sandboxing of terminals

Security on mobile terminals is mainly based on sandboxing measures that ensure the isolation of different applications.

- **How can the sandboxing of applications be implemented?**

  - The OS can ensure, via sandboxing , the strict separation of applications from each other and from the operating system, particularly in terms of memory access, but above all, in this context, permissions.
  - When the terminal is used both in private and professional life, the CNIL considers it a good practice to offer a sandboxing of personal and professional uses within the same terminal by means of technical measures and interface design is put in place. For example, the following could be permitted:
    - the use of separate user profiles within the OS, informing the user of the existence of this functionality and encouraging its use;
    - the possibility of having several simultaneous and compartmentalised instances of the same application so as to allow simultaneous use depending on the context.
  - Sandboxing by application alone is not always sufficient. The CNIL considers it a good practice to also propose partitioning between applications and the third-party codes on which they can rely, in particular in terms of obtaining permissions. In practice, giving an application permission to access a resource might not automatically extend that permission to all SDKs embedded in that application.

- **What technical measures should be implemented?**

  The CNIL considers that the following measures correspond to state-of-the-art practices:
  - make available a secure storage space dedicated to the local storage of secrets (enclave, otherwise known as 'Secure Element'), when the terminal on which the OS is executed has the necessary equipment;
  - require the encryption of network connections; failing that, report any unencrypted connection; force the use of the TLS protocol as soon as possible, or indicate its absence to users.
  - make available state-of-the-art encryption functionalities to applications;
  - make local sharing tools available between applications within the same device;

- encrypt the default backups, whether local or placed on third-party servers; keep the encryption keys only on the terminal;
- indicate state-of-the-art cybersecurity best practices that may be relevant to publishers, with examples allowing developers to identify their users' threat patterns and put in place additional security measures to address those threats, where appropriate.

2. Provide effective audit tools

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

- **What tools are available?**
  - The CNIL considers it a good practice to put in place appropriate tools (whether contained within the OS itself or offered in a development environment), which allow for a detailed analysis of network traffic, running processes, and all communications, including those made to and from the OS provider's servers.
  - Formal audit methodologies could be made available to publishers and developers to facilitate their audit of the SDKs they use in their applications and reduce information asymmetry between these stakeholders.
  - The OS provider may also offer the ability to generate simplified privacy reports, so that users can more easily understand the impacts that certain applications may have.

3. Maintaining safety over time

To ensure the security of the terminals over time, the OS provider is invited, as a best practice, to put in place processes to ensure that the user base is kept up-to-date.

- **How can the security of terminals be maintained over time?**
  - The CNIL invites the OS provider to offer users support for OS versions as long as possible over time, in particular when an update from one version to another is incompatible, in terms of material restriction, on a significant part of the current fleet of terminals.
  - The CNIL considers it a good practice to systematically offer OS security updates at least up to 7 years after the purchase of the terminal. The fact that certain functional elements are no longer compatible with the terminal is not sufficient to justify the cessation of security updates.
    - In this respect, the CNIL points out that this suggestion also falls within the criteria of the General Framework for Ecodesign of Digital Services.[54]
  - When this period has expired, the OS provider is asked to inform the users concerned of the risks associated with not updating. The provider could direct such users to alternative OSes that support its terminal and are kept secure.

8.5. Checklist

These verifications are intended to guide OS providers in the implementation of these recommendations and are presented as an indication. Some of the checks to be carried out may correspond to good practices or recommendations and not to obligations: in case of doubt, refer to the text of the recommendation.

[54] https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/

Category	Subcategory	Identifier	Description
Ensure the compliance of the processing of personal data implemented	Determine the share of the OS provider in the compliance of the processing of personal data implemented	1.1.1	An analysis of responsibilities is carried out, covering the base of the OS, the functional bricks added to it and the processing that can 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 is carried out prior to the collection of a valid consent, including at the first launch of the consent.
		1.2.2	Creating an account is not necessary to use the pre-installed OS and applications.
		1.2.3	The use of third-party notification servers is possible. Their use is optimised, particularly in terms of performance 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 availability of these tools is accompanied by clear documentation.
		1.2.5	A system of crash report and unexpected termination management in accordance with the principle of minimization is proposed, including consent to the reporting of the crash.
		1.2.6	If a remote backup system of OS settings and content is offered, it is not enabled by default. It is subject to a collection of consent and the corresponding data is transmitted and stored in an encrypted manner, using a key to which the provider of the OS does not itself have access.
		1.2.7	The availability of location data may be limited only to the use of the GPS sensor, without further processing.
Ensuring that partners are properly informed	Provide comprehensive documentation to support publisher and developer compliance	2.1.1	The documentation for third-party developers as well as the documentation for OS end-users is up-to-date, easily understandable and comprehensive and includes practical examples.
		2.1.2	Legal elements are present in this documentation and include practical examples.
		2.1.3	The various documents are available in the languages of the target audiences.
	Inform third parties of the processing operations specific to the OS	2.2.1	Partners (third-party developers and publishers, application stores, manufacturers, etc.) are able to know, understand and document, in accordance with the principle of accountability, the processing involved or induced by the use of the OS.

	Encourage the use of the most privacy-protecting features	2.3.1	The APIs proposed by the OS are documented to enable an informed decision on their use.
		2.3.2	Specific documentation is offered to developers and publishers to support them in the use of new APIs or new versions of APIs as they are more privacy-protective.
Provide tools to enable respect for users' rights and consent	Permission systems that respect the principle of data protection by design	3.1.1	Access to physical sensors, network access equipment and terminal storage space may only be made after validation of a permission by the end-user.
		3.1.2	Permissions allowing different levels of accuracy leave the choice of that level to the end user, not just to the developer of an application.
		3.1.3	Permissions can be restricted by the user, over a defined time period and number of occurrences.
		3.1.4	Users have the possibility to choose the level of information they wish to transmit as part of the permissions, in particular by manually entering the information to be transmitted. For example: transmit part of its contact book or media library rather than the whole (compartmentalisation of information).
		3.1.5	An application’s permissions are revoked when an application has not been in use for some time. The user is notified of such revocation.
	Helping to ensure proper compliance with users’ information and consent obligations	3.2.1	Permission systems allow the publisher to provide relevant information on the scope of the permission requested.
		3.2.2	Ongoing access to physical sensors is subject to a visual or audible signal within the OS interface presented to the end-user (colour badge, ringtone, vibration, etc.), allowing the user to determine which application is accessing which sensor.
		3.2.3	The user has a history of access to the aforementioned sensors, time stamped and by application.
		3.2.4	The user has a simple way to define whether a reminder is offered to him, concerning the permissions required by the applications he uses, allowing him to set a default deactivation or an information reminder of the required permissions after a certain time of non-use of his applications.
		3.2.6	Permissions can be easily revoked. Access to the menus allowing this revocation is intuitive.
		3.2.7	The OS offers data portability, within the meaning of the GDPR, allowing the user to

			migrate their data and configurations to another OS or to the same OS on another terminal.
	Protecting Minor Users	3.3.1	Parental control tools are made available to end users.
		3.3.2	These tools make a minority signal available to developers, so that the use of their applications can be restricted or blocked depending on the parameters relating to an age known by the OS.
Provide a secure platform	Ensure the security and partitioning of terminals	4.1.1	Sandboxing is implemented to limit and control interactions, memory access and permission usage between the OS and applications.
		4.1.2	A sandboxing, both technical and interface, is implemented in the OS, in order to be able to distinguish between personal and professional uses on the same physical terminal.
		4.1.3	When the terminal hardware allows it, local secret storage uses the default dedicated hardware (enclave or "SecureElement").
		4.1.4	A technical and interface constraint is applied to the implementation of network connections (e.g.: reporting unencrypted connections, outdated certificates, forcing TLS, etc.).
		4.1.5	Local inter-application sharing systems, for example via API, are made available by the OS, so that one application can securely communicate data to another application, without requiring transmission to external servers.
		4.1.6	Backups are encrypted by default, with the encryption key kept exclusively under the control of the user.
	Provide effective audit tools	4.1.1	Good security design and development practices are communicated to third-party developers.
		4.2.2	Documentation of these audit tools and methodologies is made available in order to facilitate the work of those involved in using them and to ensure that they fully understand the results observed.
	Maintaining safety 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 7 years, regardless of functional updates.
		4.3.3	When a version of the OS reaches end-of-life, clear information is provided to developers and end-users.

9. Application Store Provider Specific Recommendations

How do I read this section?

This section includes elements that are formulated as good practices and allow to go beyond compliance with the law (e.g. "As good practices, the CNIL encourages"). It also recalls the obligations imposed by the law (for example, 'the controller must') and makes recommendations to comply with them (for example, 'the CNIL recommends'). It is possible for controllers to identify alternative ways of complying with obligations, but they must then be able to justify their choice and engage their responsibility. Some elements are also formulated as good practices and allow to go beyond compliance with the law (e.g. "As good practices, the CNIL encourages").

Notice

To whom are these recommendations addressed?

- These recommendations are addressed to **application store providers.**
- The application store provider is defined as **the legal entity that develops and maintains an application store, i.e. a mobile application that indexes, highlights and enables the download of other mobile applications.** It may or may not be a commercial entity, itself potentially legally attached to another entity (manufacturer, publisher, OS provider).
- These recommendations do not apply to the store provider, apprehended as an application publisher. The **publisher of the mobile application which constitutes the application store must be subject to the same qualifications and obligations as any application publisher.** To this end, it will refer to the recommendations applicable to application publishers.
- These recommendations are specifically addressed within the application store provider:
  - the Data Protection Officer (DPO) of the entity providing the application store;
  - the legal and technical teams of OS providers, in particular manufacturers, required to authorise or integrate third-party application stores;
- These recommendations can also be consulted by mobile app publishers and developers wishing to make their apps accessible on different application 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 application store offered by default on their equipment. Regardless of the operating system used, the provider of the application store will generally not be responsible for the processing carried out within the applications themselves.
- The application store provider usually sets up a review process of the proposed applications, either for the initial publication or for the update of the application, which may lead to the publication of the application on the store or the rejection of the application, most often as part of a process allowing the publisher to modify its submission to lead to publication. It is also common for the application store provider, following reports or changes in its criteria, to suspend previously published applications.
- However, the application store provider is likely to have an influence on which apps people choose to use on their terminals. Consequently, **its design choices, the clarity of the information it offers and its ability to control the applications it makes available, before and during their availability, ultimately have an impact on the rights and freedoms of individuals in their mobile digital uses.**
- As such, it is desirable that the application store provider plays a relay role to inform users about the processing that can be implemented within distributed applications and that it implements processes that facilitate compliance with the applicable laws of published applications. **These recommendations and best practices are intended to help application store providers in this process.**

How can these recommendations be used?

- Each section corresponds to a stage in the activity of the application store provider **and sets out the privacy challenges and brings together a series of recommendations and best practices to be implemented.**
- These recommendations are without prejudice to the applicable rules on other legal grounds than the protection of personal data, in particular competition law.
- A **summary list of the main checks to be carried out** is proposed at the end of this section. Application store providers are invited to refer to it, in particular when carrying out checks prior to the publication of an application in the store, as well as when updating the store's user interfaces.

9.1. Analyze applications submitted by publishers

In the process of reviewing apps before they are published in the store, the application store provider has the possibility to collect information and analyse the proposed app in order to promote the respect of end-user's rights. The following best practices apply in particular to applications aimed at users within the European Union.

1. Centralize and analyze compliance data

In accordance with the principle of accountability, application publishers are obliged to document the processing of personal data that they will carry out in the context of the operation of the application. The application store provider may request the transmission of part of the pre-existing documentation constituted by the publisher in order to increase transparency for users.

- **What information can be obtained from each application publisher?**
  - The CNIL invites the application store provider to request the following information from the publisher:
    - the categories of data collected and the purposes pursued for each of the processing operations,
    - third parties that 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, as well as the purposes for which they are requested, as presented to the user when using the application,
    - where applicable, the third-party country in which the data will be stored and processed,
    - an update history, including update notes.
  - It is suggested that it request the provision of a contact point for privacy matters for users, as well as the privacy policy;
  - It is also suggested to allow applications to indicate whether they are aimed solely, predominantly or potentially at a minor audience.

The CNIL points out that none of the above information is confidential. They correspond to information that must be made available by the controller, as provided for in Articles 13 and 14 of the GDPR. Moreover, such data must not be used by gatekeepers in competition with business users, as provided for in Article 6-2 of Regulation 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (the Digital *Markets Act* or DMA). The CNIL invites that each of this information be provided in its most up-to-date version possible.

2. Encourage best practices in terms of privacy protection when publishing and updating applications

Due to their expertise and knowledge of operating systems, mobile application store providers appear well positioned to encourage best practices when publishing and updating apps.

- **What are the best practices to encourage application compliance?**
  - During the process of reviewing applications, whether new or updated, the CNIL invites application store providers to encourage publishers not to request blocking permissions during installation but rather to manage permissions at runtime, activating only those that will be necessary for the functionalities used by end users; To go further, the application store provider could reserve access to its store for apps that make contextual permission requests.

- The application store provider may incentivise application publishers not to use OS APIs that are too broad or outdated, in particular if the latest versions allow better compliance with data protection by design and by default principles.

- **How can I improve the update notes?**
  - Application store providers could invite publishers 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, in particular in terms of security (correction of vulnerabilities) and the implementation of additional personal data processing. The user could thus have an informed choice as to whether or not to update its application.

3. Analyze applications to detect security vulnerabilities

Application store providers shall have the ability to make analytical tools available to application publishers in order to detect possible security vulnerabilities as soon as possible.

- **How to implement static analysis?**
  - The application provider could implement static analysis before each publication or update of an application. These analysis can be automatic as well as manual and specific, in the case of applications exceeding a certain number of downloads or requiring a particularly intrusive set of permissions.

- **How can more in-depth analysis be carried out?**
  - For the most sensitive applications, the CNIL invites application store providers to conduct dynamic analysis, both automatic and manual, in order to detect abnormal behaviour in use that escapes static analysis.
  - For example, the following may be studied:
    - dynamic loading of software libraries *a posteriori;*
    - performance in the background, which may in particular have an impact on battery life;
    - the use of behaviour specific to malicious applications, documented in particular in the scientific literature, the specialised press and CVE (Common Vulnerabilities and Exposures*)* publications.

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

The CNIL encourages application store providers to act with the utmost transparency and facilitate publishers' compliance procedures. This includes communication with publishers in their respective languages. Under competition law and the DMA, where an entity alone covers several of the categories of stakeholders in that recommendation (publisher, developer, OS provider, application store provider), it is imperative that the process of verifying applications published in its application store is no more complex for third-party applications than for the applications it develops.

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

In order to support publishers wishing to send an application to the European market in their compliance with the GDPR, it is desirable that the application store review processes include the following checks.

- If the application is aimed at the European market, the publisher may be asked if the application processes personal data. In this case, the CNIL encourages the application store to check whether or not the following elements are included in the information offered to users[55], which the publisher is required to provide on the basis of the GDPR:
  - the identity and contact details of the controller and, where applicable, the representative of the controller (Articles 13(1)(a) and 14(1)(a));
  - the purposes of the processing operation and its legal basis (Articles 13(1)(c) and 14(1)(c));

[55] For example, the app store provider can ask to fill in this information in a form.

    - the period of storage of personal data (Articles 13.2(a) and 14.2(a));
    - depending on the legal basis, the existence of a means of expressing rights (Articles 13.2(b) and 14.2(b));
    - the right to send a complaint to the competent authority (Articles 13.2(d) and 14.2(d)).
  - The CNIL points out that none of the above information is confidential: they correspond strictly to the information that must be made available to the public, as provided for in Articles 13 and 14 of the GDPR. Moreover, such data must not be used by gatekeepers in competition with business users, as provided for in Article 6(2) of the DMA. The CNIL invites that each of this information be provided in its most up-to-date version possible.
  - The CNIL invites application stores to refuse applications aimed at the European market, processing personal data, which are not able to provide the above elements.
  - As a good practice, a general reminder of the legislation to be taken into account could also be made available by the application store.

2. Clearly express the expectations and processes implemented

The CNIL considers that it would be beneficial for all stakeholders if application store providers ensured the clarity, completeness and uniformity of the security and privacy requirements imposed on candidate applications, within the limits set by Article 6-12 of the Digital Markets Regulation, which states that '*the gatekeeper shall apply fair, reasonable, and non-discriminatory general conditions of access for business users to its software application stores*'.

- **What are the best practices for informing application publishers?**

  - the provision of complete documentation concerning the points of requirement studied;
  - For each of these requirements, the publication of concrete examples of problematic behaviours and solutions to address them;
  - The provision of a precise description of the validation process, the verification steps and the timescales associated with each step, including for the different remediation processes in case of rejection,
  - In the event of an update of the applicable rules, proactive communication to publishers concerning them, allocating a reasonable period for their consideration. If these updates are intended to cause previously accepted solutions to be rejected, examples of remediation techniques may also be published.

3. Facilitate the use of the tools made available

Application store providers are also invited to provide adequate tools for managing the publication process and resolving rejections.

- **Do application publishers have the tools available to publish their application effectively?**

  - The internal organizations of entities that publish applications can be very diverse.
  - As such, the CNIL encourages application store providers to allow fine-grained management of access to publisher accounts. Thus, where several stakeholders are involved 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 available?**

  - As a good practice, a communication channel between the entities publishing mobile applications on the application store and the application store provider may be established, in order to avoid blocking situations.
  - The use of the publication platform for the implementation of the rejection resolution process and subsequent communications with the organisation requesting the publication shall be preferred.

- **What are the best practices for managing refusals and suspensions of applications?**

  - Promptly inform the publisher when a security breach is detected, and in particular if this may lead to deactivation of the application or communication to end-users.

- Ensure transparent communication with mobile application publishers when applying publication validity criteria.
- Indicate the reasons for the rejection and the appeal process available to the publisher.
- Make general conditions of access available, including an out-of-court dispute resolution mechanism (DMA, Art. 6-12).

9.3. Inform users and provide them with reporting tools

The CNIL encourages application store providers to provide a sufficient level of information, including the list of third-party SDKs used by each application, to make it easier for users to exercise their rights.

1. Standardise and make available compliance data

An application store usually has a search interface that gives a summary description of each application. Each application has its own page, where a higher level of detail can be presented to inform potential users.

- **Good practices include: what information should be displayed on the pages of each application?**
  - The CNIL encourages the provision to the user of all the information referred to in section 9.1 (‘What *information can be obtained from each application publisher?*’).
  - This information could 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, for example the use of icons and tables, by choosing them in such a way as to highlight the elements with the most impact in terms of privacy protection, may be favoured.
  - The data subject must be informed of the use of personal data for commercial purposes prior to the conclusion of the contract[56]. The CNIL encourages making this information accessible to users directly within the application page.
  - The information must be presented in a neutral and contextualised manner.

- **What information should be displayed in the search interface?**
  - As a best practice, filters containing privacy criteria could be made available in the search interface. These could relate to the use of certain permissions, the collection of certain data or even to a ‘score’ relating to privacy criteria.
  - Also as a best practice, and if the creation of such a score is envisaged, it should be based on a methodology defined in advance, in a transparent manner, by a third party to the application store provider and ideally agreed between the different stakeholders of the ecosystem and civil society. The process of calculating that score should also be entrusted to a third party, or alternatively be subject to certification by a third party, in particular to ensure that it fulfils its transparency objectives. The provision of source data for the calculation of this score in an open and easily exploitable format, so that alternative methodologies can be proposed, is encouraged. In that regard, it is recalled that, under Article 6(5) of the DMA, the gatekeeper ‘*shall not treat more favourably, in ranking and related indexing and crawling, services and products offered by the gatekeeper itself than similar services or products of a third party. The gatekeeper shall apply transparent, fair and non-discriminatory conditions to such ranking’*.
  - The CNIL recalls, in the event of the implementation of such a score, that applications published by stakeholders that also provide operating systems and/or SDKs should be subject to the same rules as third-party applications, under the applicable competition law.

2. Make clear reporting arrangements available

The application store interface is a privileged channel to allow user feedback to be taken into account.

- **How can feedback and reports from users be used?**

[56] Application publishers are obliged to provide the consumer (here the user of the application) with the pre-contractual information provided for in Article L. 221-5 of the Consumer Code, resulting from the transposition of Directive 2011/83 on consumer rights, including information on the essential characteristics of the good, service, digital service or digital content (Consumer Code, Art. L. 221-5 I 1°).

- In accordance with Article 16 of the Digital Services Act (DSA), hosting service providers, including application store providers, shall '*put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content*'.
- The CNIL recommends that application store providers include in this mechanism the possibility of reporting practices that may be contrary to the GDPR, which may fall within the scope of illegal content as defined in Article 3.h of the DSA (for example: failure to exercise rights, failure to comply with obligations relating to the collection of consent, including through the use of misleading designs or dark patterns[57], execution of SDK functionalities without prior consent, presence of unsupervised transfers, etc.).
- Those reports could, as a good practice, be used to guide the checks carried out by the store on the applications it hosts.

3. Notify in case of vulnerability detection or need to update

The application 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 CNIL encourages the application store provider to establish a protocol in case vulnerabilities are revealed in a widely deployed application or SDK.
  - In particular, the application store provider may implement analyses (including static analyses) to determine which applications are affected by a vulnerability.
  - Once vulnerable applications are detected, several measures can be applied:
    - suspend automatic updates of all or part of the user application pool;
    - temporarily remove all vulnerable applications, making it impossible to download them and protecting potential and future users, as long as they have not been updated and this update does not pass the security test established when detecting vulnerable applications.
  - The application store provider could also analyse whether user information is needed. If the vulnerability creates high risks for data subjects, for example, it may be considered to display a system notification to users that one or more of their applications are vulnerable.

9.4. Checklist

These checks are intended to guide application store providers in the implementation of these recommendations and are presented as an indication. Some of the checks to be carried out may correspond to good practices or recommendations and not to obligations: in case of doubt, refer to the text of the recommendation.

Category	Subcategory	Identifier	Description
Analyze applications submitted by publishers	Centralize and analyze compliance data	1.1.1	Elements relating to the processing, permissions requested or third parties accessing the data are requested for their provision during the application review process.
		1.1.2	A privacy policy and a contact point are defined and accessible to end users, for each application publisher with at least one application published in the store.

[57] Excluding practices covered by Article 25 of the DSA.

		1.1.3	Where an application is intended solely, predominantly or potentially for a minor audience, this information is indicated in the store page relating to that application.
	Encourage best practices in terms of privacy protection when publishing and updating applications	1.2.1	During the review process, publishers are advised not to request bulk permissions during installation and are encouraged to have runtime permissions management.
		1.2.2	The application store provider may encourage app publishers not to use OS APIs that are too broad or outdated
		1.2.3	Publishers are invited to publish informative update notes for users so that they can assess the need for the update.
	Analyze applications to detect security vulnerabilities	1.3.1	Static analyses are performed on each new application or application version, before any publication in the store.
		1.3.2	Dynamic analyses are performed on more sensitive applications to detect abnormal behaviors.
Implement transparent application review processes that incorporate verification of basic data protection rules	Integrate verification of basic data protection rules into application review processes	2.1.1	In the event that the application processes personal data, the presence of the following elements in the information to users is checked: • the identity and contact details of the controller • the purposes of the processing and its legal basis • the retention period of personal data • according to the legal basis, the existence of a means of expressing rights • the right to send a complaint to the competent authority
		2.1.2	Applications aimed at the European market that are unable to provide these elements are not published in the application store.
	Clearly express the expectations and processes implemented	2.2.1	Application publishers is properly informed, in particular on the elements of compliance incumbent on them according to the store’s criteria. The update of these elements, in time, is communicated to them.
	Facilitate the use of the tools made available	2.3.1	Fine management of access to the publisher accounts of the application store is proposed, so that several users can have a separate use of repositories, version signatures, update notes.

		2.3.2	A clear channel of communication between entities publishing mobile applications and the application store is displayed, favouring a channel built into the application store itself.
		2.3.3	Refusals to publish and the corrective measures to be applied to remedy that refusal, as well as any appeals, is clearly indicated to the publishers and is based on the relevant documentation.
Inform users and provide them with reporting tools	Standardise and make available compliance data	3.1.1	All privacy-related information, transmitted by publishers or known to the store, is available to the end user before purchase or download.
		3.1.2	All information required or useful for the end-user is displayed in a format appropriate to the system in which it is accessed.
		3.1.3	Privacy filters are available among the search options.
	Make clear reporting arrangements available	3.2.1	End users have the ability to report applications that do not meet their obligations, directly from the store.
	Notify in case of vulnerability detection or need to update	3.3.1	A protocol is defined concerning 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 application page in the store, on a potential security risk.

10. Glossary

Mobile application

The concept of a mobile application refers to application software distributed in the environment of smartphones and tablets.

These applications are run in isolation (or in sandbox mode) by an operating system that limits the functionality they can access via a permissions system.

Software Development Kit or SDK

The *software development kit* (SDK) 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 make it possible to facilitate or speed up the development of software features, avoiding the developer from writing the entire code of the application.

These SDKs are usually integrated by adding the code offered by them in the developed application, code that will eventually allow to interface with the infrastructure of the SDK provider to implement the functionality. They cover many functionalities, but the most common are audience analytics, advertising selection and delivery or e-commerce functionalities.

Sandboxing mode

Execution in sandboxing mode is a security mechanism implemented by an operating system to isolate an application running vis-à-vis the core of the operating system, but also other applications running on the terminal (computer, mobile, etc.).

This isolation reduces the risk that could be linked to the misuse of terminal functionalities, but also to attempts by an application to access data or disrupt the operation of a third-party application.

In general, applications running in sandbox mode have rather reduced default functionalities, having the possibility to use only APIs provided by the operating system, with the user's permission.

Application Programming Interface (API)

An API (application programming interface*)* is a software interface that allows a software or service to be linked to another software or service in order to exchange data and functionalities.

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. Access can be free or paid.

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

Operating System (OS)

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

In the context of mobile applications, the operating system 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* by the user) and the terminal. In particular, it implements the 'sandboxing' execution of applications, as well as the permission system allowing access to the terminal's functionalities.

Access Permission

Access permissions are devices implemented by the operating systems (OS) of mobile terminals to allow users to choose which features are accessible to mobile applications.

Those mobile applications have only limited access to those features by default, for security and privacy reasons. The operating system therefore provides them with APIs allowing them to make queries in order to be allowed additional functionalities, provided that the user accepts it via an interface provided by the operating system.

There are in practice different types of permissions. Technical permissions are thus intended to grant or block access to certain protected resources, irrespective of the purposes for which access to those resources is requested. Other permissions are intended to authorise or refuse the carrying out of certain actions for a specific purpose, through access to certain resources but also by other means.

Audience *measurement ('analytics')*

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

Advertising ID

Advertising identifiers are digital identifiers, often represented in the form of strings, generated and associated with a terminal by the operating system (OS), and which may, under certain conditions depending on the operating system in question, be made available to applications that request them.

These identifiers are specifically designed to allow the identification of a single user by different applications, identification made impossible outside of it by the execution in sandboxing mode of the applications.

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 apps embed the targeting module of that social network, access to the advertising ID will allow the person's profile data to be used to target advertising in the context of those third-party apps.

Geolocation

Geolocation is a technology used to determine the location of an object or person by returning the result in the form of geographical coordinates. The technology usually relies on the GPS system or communication interfaces of a mobile phone, and can return results with varying accuracy. The applications and purposes of geolocation are multiple: assistance with navigation, connecting people, but also real-time management of the staff and vehicle resources of companies, etc. This technique is part of the more general group of location techniques, but these can go beyond the concept of geolocation, for example by returning the locality rather than the geographical coordinates.