BCLP. Client Intelligent

Insights

MOBILE APPS: WHAT DOES THE CNIL RECOMMEND FROM A PRIVACY PERSPECTIVE?

Feb 17, 2025

SUMMARY

While mobile apps have become one of the major means of access to digital services, their ubiquity is accompanied by significant risks to users' privacy, due to the massive amount of personal data they collect and process. Last September the *Commission Nationale de l'Informatique et des Libertés* (CNIL) published a set of recommendations to improve compliance of mobile apps with data protection rules. These clarify the obligations of the various stakeholders and set out best practices in the mobile app ecosystem. The recommendations are structured to distinguish between requirements which are mandatory and those which are best practice and are arranged by category of the entity involved in the mobile app value chain, with practical checklists for assessing and documenting compliance. We unpack the key recommendations by the five main categories:

- publishers;
- developers;
- software development kit (SDK) providers;
- operating system (OS) providers; and
- app stores.

There are specific recommendations for each category of entity, tailored to its role in the lifecycle of an app, from development to publication on an app store. The French competition authority (the ADLC) also gave its opinion on the recommendations, expressing concern about the risks that these recommendations could create for competition, to the benefit of vertically integrated players, which dominate the market for operating systems, app stores and various related services. These closed ecosystems could exploit compliance with data protection rules to reinforce their dominance, by imposing high compliance standards that only a few companies would be able to easily meet, and which would therefore act as a barrier to market entry for smaller players. The CNIL therefore

adjusted its recommendations to ensure that they do not create disproportionate advantages for these dominant companies, to the detriment of other market players.

STAGE 1: IDENTIFYING YOUR ROLE AND SCOPE OF THE DATA PROCESSING

As a first step, each entity involved in the lifecycle of an app must determine the role it plays in the app value chain. It must then consider its role in relation to the personal data it processes. This assessment consists of determining, for each data processing operation, whether the actor is acting as data controller (or joint controller) or data processor. This is made more difficult where a party occupies two or more roles simultaneously (for example, where an app store provider also publishes some of the applications it distributes). In addition, it may act as data controller for some processing operations, and as data processor for others.

STAGE 2: TAILORED RECOMMENDATIONS BY ROLE

The CNIL has provided specific recommendations tailored to the responsibilities and functions of each entity, setting out both the general obligations applicable to all data controllers and processors and providing practical examples.

1) PUBLISHERS

They must first identify all the personal data processing operations that will be carried out when the app is used, to determine the purposes of each processing operation and to identify the appropriate legal basis. For data processing undertaken for advertising or content recommendation purposes, the user's explicit consent is required, particularly for operations on the user's terminal. However, no consent is required for processing that is strictly necessary when an online communication service is expressly requested by the user.

Several key principles should guide the publisher in the app design phase (e.g. minimisation of data, limited retention period). In addition, when applying the concept of privacy by design, publishers must configure the app's default settings in such a way as to be as non-intrusive as possible. It must also document and justify these choices to comply with the principle of accountability. Publishers must also have contractual arrangements in place with their partners, particularly developers, who act as subcontractors (defining the respective responsibilities of the publisher and the developer). The CNIL also stresses the importance of properly managing access permissions to phone resources (location, contact list, camera, etc.). App users must always be able to control access and give explicit authorisation via their OS.

In the development phase, the publisher must carry out a rigorous analysis to determine:

- If access to certain data is strictly necessary for the operation of the app;
- If an alternative solution exists to avoid the need for certain user ; and
- If the data can be stored locally on the user's terminal, rather than on external servers.

Only strictly necessary data should be requested. The publisher must also ensure that the user is fully informed of the purposes for which the data is collected and the type of processing involved. This information can be provided, for example, by means of a clear privacy policy that is accessible even before the app is downloaded.

Finally, to facilitate the exercise of rights of access, rectification and deletion, the CNIL recommends setting up a rights management center within the app. It also suggests, as a good practice, offering an automated system for responding quickly to user requests, for example via a dedicated API.

2) DEVELOPERS

Although the developer acts as the publisher's subcontractor in the development of the app, it must advise the publisher to ensure that appropriate data protection mechanisms are integrated from the design phase. This involves design advice on minimizing the impact of the app on users' privacy, and implementing the appropriate mechanisms for obtaining valid consent from users where necessary, as well as advice about functionality (and use of technical tools (such as SDKs). Although the final choice of SDKs rests with the publisher, as data controller, the developer must ensure that it offers solutions that comply with the requirements of the GDPR. Under no circumstances may the developer engage a subcontractor to process data without the publisher's prior written approval.

3) SDK SUPPLIERS

Suppliers of SDKs provide developers and publishers with essential tools for integrating advanced functionalities into apps. These suppliers will be data controllers, joint data controllers or data processors depending on the nature and scope of the processing they carry out. The design of an SDK must incorporate the fundamental principles of the GDPR from the outset. The SDK supplier also has a role in advising publishers and developers, providing them with clear technical and legal documentation on how the SDK handles data. This documentation must include the information necessary for editors and developers themselves to demonstrate their compliance with the requirements of the GDPR, particularly in terms of determining purposes, setting retention periods and data security.

4) SUPPLIERS OF OPERATING SYSTEMS

Operating system (OS) vendors provide the basic platform on which apps are installed and run. As such, they are responsible for building data protection mechanisms into their system from the outset, while offering functionality to publishers and developers that enables them to comply with GDPR.

The OS supplier designs the phone's permissions management system, which enables users to manage each app's access to the device's various functions and data. Users must be given granular control of permissions so they can control their personal information. For example, permissions should be used to restrict access to the device's sensors (camera, microphone, GPS), network functions (Bluetooth, Wi-Fi) and storage (photo gallery, contacts). The CNIL also recommends that OS suppliers provide parental control functions that allow permissions and content to be adapted according to the user's age. These parental controls, which should ideally be stored locally, enable parents to restrict access to certain apps or functions.

5) APP STORE PROVIDERS

App stores providers act as intermediaries, offering publishers a distribution platform and users a place to download mobile apps. Although an app store is not responsible for the processing carried out within the apps themselves, it exercises significant indirect control by virtue of its ability to accept or refuse the listing of apps in its store on the basis of criteria that it defines. This control, combined with the criteria it uses to classify and present apps, gives it significant influence over users' choices and, consequently, an indirect impact on their rights and freedoms.

Whilst the CNIL had initially envisaged a stronger monitoring role for app stores, this has been limited, in response to ADLC feedback, so that dominant platforms do not take advantage of this privileged access to publishers' commercial information (for example, specific processing purposes or business models). The CNIL has also adjusted its recommendations concerning the introduction of a privacy protection score for each application, with the ADLC recommending that the score is drawn up by a regulator, a public body or an independent third party, following criteria of transparency, objectivity and proportionality. The CNIL therefore requires that the score is defined by an impartial and transparent methodology, developed in collaboration with various stakeholders, and excluding app store providers from the calculation of the score. The CNIL also specifies that, for companies that combine several roles (publisher, OS supplier, application store manager), this review process must not be more complex for third party apps than for their own, in compliance with the DMA. Note that there are additional requirements for platforms which qualify as gatekeepers (under Articles 6(2), 6(5) and 6(12) of the DMA), which impose fair, reasonable and non-discriminatory access conditions to an app store.

The CNIL also recommends that app stores make all information relating to the processing of personal data available to users directly on the relevant page. Although the publisher must fill in and update this information, the app store can provide a function to centralise this data. App stores must also offer reporting tools and make it easier for users to exercise their rights (right of access, rectification, deletion, etc.).

The mobile app sector is a particular focus for the CNIL and these new guidelines are in line with the priorities announced by the CNIL in 2023, which identified user tracking by mobile apps as one of its main targets. In addition, as part of its 2025-2028 strategic plan, the CNIL announced that it would be conducting a major campaign from spring 2025 onwards, to ensure all players in the mobile app sector comply with these rules.

Speak to us: BCLP's Data Protection team will support you as you develop innovative technological solutions to ensure these are compliant with data protection rules.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21

consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.