As the CNIL publishes the final version of its recommendations on mobile applications, the Autorité publishes the opinion issued to the CNIL in December 2023 as part of the preparation of its recommendations

Published on September 24, 2024

Background

Mobile applications are one of the main ways of accessing digital content and services from smartphones and tablets. The use of apps involves the processing of large quantities of personal data. Against this backdrop, the draft recommendations prepared by the French data protection authority (*Commission nationale de l'informatique et des libertés* – CNIL) aim to provide greater legal certainty for stakeholders and promote best practices for the benefit of users.

The *Autorité* welcomes the CNIL's draft recommendations, insofar as they aim to meet the need for clarification expressed by players in the sector and, ultimately, to promote greater protection of users' personal data. Furthermore, the *Autorité* considers that better information on the implementation of privacy regulations leads to market transparency and reduced barriers to entry.

However, the *Autorité* would like to comment on the competition issues that may be raised by the CNIL's draft recommendations as a whole and, more specifically, by specific provisions concerning certain categories of players. Consequently, the *Autorité* is making a series of recommendations to the CNIL.

Generally speaking, the *Autorité* believes that privacy measures that go beyond what is strictly imposed by the General Data Protection Regulation (GDPR) are not

unlawful *per se*, but may be detrimental to the economic efficiency of the markets. For this reason, they must be defined and implemented in such a way as to avoid generating anticompetitive effects that would not be counterbalanced by sufficient gains for consumers.

To this end, the *Autorité* calls on the CNIL to take the competitive structure of the sector into account in its approach, in particular the position of certain players. Specifically, the *Autorité* calls on the CNIL to be particularly attentive in ensuring that its recommendations do not risk strengthening the strong market power of certain players, notably those that have been designated as gatekeepers for certain services or that could be considered to be in a dominant position, as these players could use the recommendations for anticompetitive purposes.

Lastly, as the best practice recommendations are the sole initiative of the CNIL and not a result of obligations imposed by the regulations in force, the *Autorité* calls on the CNIL to ensure that its recommendations do not create barriers to entry into the French market, or disadvantages in terms of costs or constraints for companies established in France.

The background and the CNIL request

For the first time, the French data protection authority (*Commission nationale de l'informatique et des libertés* – CNIL) asked the *Autorité de la concurrence* to issue an opinion on draft recommendations on mobile applications (hereafter "mobile apps"). This request reflects the commitments made by the two authorities as part of the joint declaration adopted in December 2023[1] and marks a new stage in the deepening of their relationship (see the joint declaration by the *Autorité* and the CNIL on regulatory synergies).

Mobile apps, application software distributed in the smartphone and tablet environment, are one of the main ways of accessing digital content and services from mobile terminals. They are used to add extra functionalities or services in a wide variety of areas (social networks, entertainment, remote shopping, mobility,

banking services, etc.). The use of apps involves the processing of large quantities of personal data. According to the CNIL, while the principles and obligations of data protection and privacy are now well known to website operators, and are already the subject of recommendations, there can sometimes be uncertainty around their implementation in the context of mobile apps.

To overcome this uncertainty, the CNIL's draft recommendations aim to provide greater legal certainty for stakeholders and promote best practices for the benefit of users. In particular, they clarify the qualifications and responsibilities of the different players in the mobile app ecosystem with regard to the applicable privacy regulations. First, the draft recommendations recall the main obligations of the players in the sector with regard to the General Data Protection Regulation (GDPR) and the French Data Protection Act (***Loi informatique et libertés***)[2]. Second, they include a series of tips and best practices recommended by the CNIL.

In this context, the objective of the CNIL in consulting the ***Autorité*** was to ensure that its recommendations effectively protect users' personal data without hindering free and undistorted competition, which guarantees innovation and diversity on the mobile app market. The ***Autorité*** is pleased to note that its recommendations have been taken into account by the CNIL in its final recommendations (in French).

The competitive structure of the mobile app sector

The competitive structure of the mobile app sector is characterised by the presence of multiple players involved at the various stages of the mobile app value chain, from design to distribution to users. The sector is also marked by the presence of vertically integrated players throughout the value chain (Google[1] and Apple).

The five categories of players in the mobile app value chain are as follows:

- ***Software developer kit (SDK) providers***, which offer a range of tools used for app development, depending on the operating system used. The

widespread use of SDKs is largely due to the fact that they often facilitate or accelerate the development of software functionalities, avoiding the need for the developer to write the entire app code.

- ***Developer***, which designs and builds the app on behalf of the publisher, based on the latter's specifications.
- ***App publisher***, which makes the app available to users (usually via one or more app stores) in order to offer its products or services. The app publisher also defines the business model and, in particular, sets the price.
- ***Operating system (OS) provider***, which provides the operating system[5] specially configured and installed on the user's mobile terminal, the environment in which the app will subsequently run. The two main operating systems for mobile phones are those of Apple (iOS) and Google (Android).
- ***App store provider***, which provides an online app distribution platform, in the form of an app accessible on the user's terminal from a compatible operating system (e.g. the App Store for a terminal running Apple's iOS operating system, or the Play Store for a terminal running Google's Android operating system). The app store provider is often, but not always, the operating system provider.



The *Autorité* notes that players such as Google and Apple are present at all levels of the value chain as OS, app store and SDK providers, as well as publishers, developers and providers of other services. These vertically integrated players have set up distinct ecosystems, in which they establish specific access rules in their capacities as OS and/or app store providers. In addition, these players are likely to hold dominant positions in certain markets in the value chain and have recently been designated as “gatekeepers” within the meaning of the Digital Markets Act (DMA) by the European Commission for several core platform services, including their operating systems for mobile terminals (Google Android for Alphabet and iOS for Apple) and their app store intermediation services (Google Play Store for Alphabet and App Store for Apple).

The *Autorité* welcomes the CNIL's draft recommendations and proposes recommendations to address its competition concerns

The *Autorité* and the CNIL share a common ambition to protect personal data and privacy and respect competition. In particular, there is a certain convergence of objectives between their policies, in that both are implemented for the benefit of users.

However, the *Autorité* highlights that while the interplay between competition and privacy protection can be a source of synergy, it can also be a source of tension. First, the accumulation of data by certain companies helps to establish the market power of those companies and requires particular vigilance on the part of competition authorities. Second, the level of protection afforded to user data can be a real competitive parameter, just like price, particularly if this protection exceeds the level imposed by personal data protection regulations.

Lastly, the *Autorité* specifies that while privacy measures that go beyond what is strictly imposed by the GDPR are not unlawful *per se*, they may be detrimental to the economic efficiency of the markets. For this reason, they must be defined and implemented in such a way as to avoid generating anticompetitive effects that would not be counterbalanced by sufficient gains for consumers.

The general recommendations made by the *Autorité*

In its opinion, the *Autorité* makes several preliminary observations on the general competition issues that may be raised by the CNIL's draft recommendations, which could contribute to the drafting of the text.

In particular, the *Autorité* welcomes the application of competition law in Sections 8 and 9 of the CNIL's draft recommendations, but considers that competition law should be taken into account throughout the CNIL's draft recommendations.

Second, the *Autorité* invites the CNIL to review the role granted to OS providers and app stores in its draft recommendations. These operators, which are already in an asymmetrical position, are granted an important privacy protection role by the draft recommendations, which does not derive directly from obligations imposed by the personal data protection regulations in force, in particular the GDPR.

Accordingly, the *Autorité* invites the CNIL to ensure that its recommendations do not confer additional power on players that already enjoy strong market power, notably those that could be considered to be in a dominant position and could use the recommendation for anticompetitive purposes.

The *Autorité* also calls on the CNIL to expressly state that its recommendations apply in the same way to the proprietary mobile apps of OS and app store providers as to third-party apps, in order to avoid its recommendations being used by certain operators to implement differentiated treatment that could give proprietary mobile apps an advantage.

The *Autorité* also notes several contradictions between the CNIL's draft recommendations and the DMA, not only with regard to the powers conferred on gatekeepers but also in terms of certain specific provisions.

The *Autorité* calls on the CNIL to take particular care to ensure that its recommendations do not have the effect of delegating its jurisdiction, as national regulator, to gatekeepers, at the risk of reinforcing market power asymmetries to the benefit of the latter.

In addition, the *Autorité* learned during the interviews organised for the purpose of the opinion that only entities with a head office in France would be monitored by the CNIL. The CNIL's recommendations could therefore create additional constraints for French players, impacting their competitiveness.

> The *Autorité* calls on the CNIL to take particular care to ensure that its recommendations do not create additional barriers to entry for new entrants to the French market, or disadvantages in terms of costs or constraints for companies established in France.

The specific recommendations made by the *Autorité*

Without conducting an exhaustive analysis of the CNIL's draft recommendations, the *Autorité* also makes recommendations on certain provisions specifically concerning categories of players in the mobile app value chain.

Among these recommendations, the *Autorité* addresses in particular the competitive concerns that could be raised by the provisions concerning OS providers and app stores.

In its draft recommendations on mobile apps, the CNIL gives OS providers and app stores an important role in protecting privacy, which does not result from obligations imposed by the regulations in force. It is therefore essential to ensure that its recommendations cannot be used by OS providers and/or app stores for anticompetitive purposes (e.g. discriminatory treatment) and do not lead to the undue creation of barriers to entry that would reinforce existing asymmetries in

certain already concentrated markets in the value chain.

OS providers

With regard to information and advice to partners, the *Autorité* would like to draw the CNIL's attention to the fact that the implementation of its draft recommendations, insofar as they invite OS providers to provide advice and complete legal documentation, could enable OS providers to impose their way of complying with regulations on players in the value chain and, under the guise of better protecting privacy, introduce rules that reduce competition in the market.

> While supporting the objective of providing good information to players in the mobile app value chain, a source of market transparency, the *Autorité* draws the CNIL's attention to the role granted to OS providers and, at the very least, calls on the CNIL to specify that the documentation provided must not have the value of legal advice or aim to impose a way of complying with European regulations.

With regard to OS providers' permissions to access user terminals' sensors, functionalities or storage and their use to enhance privacy protection, the *Autorité* stresses that this objective goes beyond mere compliance with personal data protection regulations, and makes recommendations on a range of subjects. In particular:

The *Autorité* invites the CNIL to clarify certain provisions of the sections on the implementation of a permissions system, in particular with regard to the scope of the resources concerned, the accessibility of publishers to OS resources not subject to permission, and the respective responsibilities of OS providers and publishers. In addition, the *Autorité* invites the CNIL to specify the conditions for implementing the provision on the end of support for the most problematic functionalities.

Furthermore, with regard to all these provisions, and insofar as the use of permissions recommended by the CNIL does not result from the direct implementation of the personal data protection regulations in force, the *Autorité* draws the CNIL's attention to the fact that its recommendations must not confer excessive discretionary power on certain vertically integrated players, such as OS providers. To this end, the *Autorité* considers that privacy protection must not hinder competition, which means avoiding a situation where access to any given phone functionality becomes subject to permission, to the detriment of the diversity of supply and innovation. At the very least, the *Autorité* invites the CNIL to clarify that OS providers are required to apply proportionate, objective, transparent and non-discriminatory permissions, which therefore apply uniformly to all apps, whether pre-installed or not and proprietary or not.

Mobile app store providers

In its draft recommendations, the CNIL recommends in particular that app store providers conduct an analysis of the apps submitted by publishers to be listed in their app stores, implement transparent app review processes that include the verification of basic data protection rules, and provide users with information so that they can more easily exercise their rights.

To this end, the *Autorité* would like to draw the CNIL's attention to the need to ensure that its recommendations concerning app store providers do not hinder the competition that may exist between players present at the various stages of the value chain, or with regard to potential entrants.

In addition to this general remark, the *Autorité* draws the CNIL's attention to several specific provisions in the section on to app store providers.

For example, with regard to the collection of information recommended by the CNIL for the review of mobile apps, the *Autorité* expresses doubts about the communication of commercially sensitive information. The collection of this information and the analysis of competitors' apps by vertically integrated operators could give these operators access to potentially useful information for improving their own apps or launching new competing apps, and reinforce the asymmetry of information to their advantage.

> The *Autorité* invites the CNIL to clarify that the data is collected from publishers on a declarative basis, the recommendations do not imply that app store providers are responsible for verifying the accuracy of the data, and the data transmitted to app stores must exclude any commercially sensitive information.
>
> In addition, the CNIL could also usefully point out the obligations incumbent on Google and Apple as "gatekeepers" for app stores, in particular the ban on using the data of competing user companies, collected as part of the activity covered by the DMA for use in another market, as laid down in Article 6(2) of the DMA.

With regard to compliance analysis, several of the players interviewed fear that, under the guise of the implementation of the CNIL's draft recommendations, the provisions concerned will enshrine review processes that are already causing them difficulties. The *Autorité* recalls that an operator, including one in a

dominant position, is free to lay down the rules that it deems useful for conditioning access to its goods or services, provided that the implementation of those rules does not have the object or effect of restricting competition. However, the *Autorité* draws the CNIL's attention to the fact that its recommendations must not have the effect of delegating its regulatory missions to app store providers, insofar as this could distort competition in the markets concerned or confer additional market power on these vertically integrated players.

> The *Autorité* invites the CNIL to limit its recommendation on compliance analysis to the specific obligations of these players that result from the regulations in force, specify that, at the very least, the checks should be performed for all apps subject to store review as well as for pre-installed apps, including proprietary apps, and specify the importance of having a review process that guarantees transparent, fair and non-discriminatory access conditions based on proportionate criteria and providing for dialogue between the parties, especially a dispute resolution mechanism.
>
> In this respect, the *Autorité* points out that such obligations appear to fall under Article 6(12) of the DMA applicable to gatekeepers.

Furthermore, with regard to potential barriers to entry and expansion for alternative app stores, the App Store is, to date, the only app store authorised by Apple on Apple mobile terminals, and the Play Store is the main app store used on mobile terminals running the Android operating system. Competition from the stores of certain mobile manufacturers (such as Samsung) and open-source stores (such as F-Droid) remains weak.

The *Autorité* invites the CNIL to clarify the terms of application for existing and potential alternative and small-scale app stores so that its recommendations do not represent a barrier to entry or survival for the latter.

Lastly, the *Autorité* also comments on the provisions of the CNIL's draft recommendations on the implementation by app store providers of filtering or scoring criteria for privacy protection. In particular:

The *Autorité* calls on the CNIL to specify that a scoring system can only be created by the regulator or the French government, or by an independent third party, based on proportionate assessment criteria and data collection requirements. Furthermore, such systems may only be implemented by potentially dominant companies in an objective, transparent and non-discriminatory way and may only be implemented by platforms designated as gatekeepers in compliance with the provisions of the DMA.

Lastly, the implementation of a scoring system could be subject to a label or certification process by an independent third party in order to ensure the reliability of the indicator. While an app store may usefully propose a system for making reports, all reports received should be sent to the CNIL, the competent authority for judging compliance with personal data protection regulations on French territory and, where appropriate, for issuing sanctions.

[1] "Data protection and competition: a common ambition", a joint declaration by the *Autorité de la concurrence* and the CNIL (December 2023).

[2]French law 78-17 of 6 January 1978 on information technology, data files and civil liberties.
[3]Alphabet Inc.
[4]To use an app, the user runs the app on their mobile terminal via its operating system (OS) specially configured and installed on their mobile phone or tablet. The OS defines and supports all authorised interactions between the user and the terminal, as well as between third-party mobile apps (those installed later) and the terminal.

Joint document on close cooperation between the CNIL and the Autorité de la concurrence on mobile applications

CNIL recommendations on mobile applications: close cooperation with the Autorité de la concurrence to reconcile respect for privacy and a dynamic competitive environment (in French)

OPINION 23-A-20 OF 4 DECEMBER 2023

on the draft recommendations prepared by the CNIL on mobile applications

See the full text of the opinion (in French)

Contact(s)

Nicola Crawford
Communications Officer
+33155040151
Contact us by e-mail