The President

[redacted]

Paris, on

Our ref.: [redacted]
To be recalled in all correspondence
Registered letter with acknowledgement of receipt XXXXX

Dear Sir,

The main activity of the company [redacted] is the production of an air management simulation video game called '[redacted] The game is used by users residing in France and in several EU countries.

In accordance with my **decision no 2024-130C of 28 June 2024**, the Commission nationale de l'informatique et des libertés (CNIL) carried out, on 24 April 2024 an online inspection of the websites "[redacted]" and "[redacted]" and the mobile applications "[redacted]" and "[redacted]". This investigation continued with a questionnaire sent on 21 August 2024.

The purpose of this investigation was to verify whether the processing of personal data by your company comply with the provisions of Regulation (EU) 2016/679 on data protection ('the GDPR') and with the Law of 6 January 1978 as amended (French Data Protection Act).

The findings made during those checks, and the additional information provided on 22 September and 6 December 2024, lead me to note the following facts.

I. Analysis of the facts in question

1. On the breach of the obligation to store personal data for no longer than necessary

In law, Article 5(1)(e) of the GDPR provides that personal data must be kept for "*no longer than is necessary for the purposes for which* [they] *are processed*".

In the present case, the company [redacted] states that it retains the data of the users of the '[redacted]' game for a period of three years from their last connection.

However, the delegation noted the presence of personal data in an extract of data relating to inactive users (i.e. not connected to the game for at least three years).

Therefore, I consider that the company [redacted] infringed the provisions of Article 5(1)(e) of the GDPR by retaining the data of inactive users for a period exceeding that which it itself considered necessary in the light of the purposes for which they are processed.

However, I take good note that your company has informed the delegation about the deployment of an automated deletion tool in order to delete the data of inactive users for three years.

2. **On the breach of the obligation to communicate transparent information**

In law, Article 12(1) of the GDPR provides that "*the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14* [...] *relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form*".

By way of illustration, the Article 29 Working Party ('G29', now the European Data Protection Board (EDPB)) states in its Guidelines of 11 April 2018 on transparency within the scope of the GDPR that the criterion "*easily accessible*" "*means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed*" and that "*a central consideration of the principle of transparency* [...] *is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used*". It recommends, as a good practice, that "*at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected*".

The Guidelines also state that information "*should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use*". The Guidelines also state that "*the data subject must not have to actively search for information covered by* [Articles 13 and 14] *amongst other information, such as terms and conditions of use of a website or ap*p".

In that regard, the Commission considers that information relating to the protection of personal data of data subjects does not meet the requirements of transparency and accessibility laid down by the GDPR where that information is accessible solely from the links entitled "General conditions" and "Legal information". In view of the wealth of information to be mentioned under the various laws, those arrangements do not allow the user to receive sufficiently clear and accessible information on the processing of his or her data. (CNIL, P, 1 December 2021, Order, Company X, No MED-2021-131, not published)[1].

In the present case, the delegation noted that the website "[redacted]" includes a link to General Conditions of Use ("CGU") (in French) containing a link called "Privacy Policy" (in English in the text). To access this information from the account creation page, the user must click at the bottom of the page on a link "CGU" and then on a "Privacy Policy" link (in English in the text).

By clicking on this link, the user has access to data protection information in French. Finally, on the mobile applications "[redacted]" and "[redacted]", the delegation noted the presence of a link "Terms and privacy policy" (in French) which refers to the CGUs containing a link "Privacy policy" (in English in the text).

[1] Cf. « Table et informatique » (https://www.cnil.fr/sites/cnil/files/202312/tables_informatique_et_libertes.pdf).

It follows that information relating to the protection of personal data is not easily accessible to users when collecting their data for the creation of an account, as they must actively seek that information among other, more general, information. The presentation of information relating to the protection of personal data accessible from an English-language link in the general conditions of use cannot be regarded as satisfying the requirements of easily accessible and transparent information.

Therefore, I consider that the company [redacted] infringed the provisions of Article 12 of the GDPR by not providing transparent, comprehensible and easily accessible information within the meaning of the abovementioned provisions of the GDPR.

3. On the breach of the obligation to ensure an appropriate level of security

In law, Article 32 of the GDPR requires the controller "*taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,* [to] *implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

In its recommendation on passwords and other shared secrets[2], the CNIL recalls that "*any password useful for the verification of authentication must be transformed in advance by means of a specialised, non-reversible and secure cryptographic function (i.e. using a public algorithm deemed strong whose software implementation is free of known vulnerability), incorporating a 'salt' and cost parameters in time and/or memory necessary for its attack*".

In its recommendations on multifactor authentication and passwords[3], the ANSSI states that "*the recommended cryptographic hash functions, such as the SHA2 family, are very quick functions to perform, which, in the context of password storage, is an advantage for attackers, allowing them to test (i.e. to calculate fingerprints) many passwords*". It therefore recommends the use of algorithms whose parameters make attempted attacks costly in time and memory, citing scrypt and Argon2 functions by way of example.

In the current state of the art, the Commission has developed specific recommendations in its guide for developers, recommending to store passwords "*in the form of hash using a proven algorithm, such as Argon2, yescrypt, scrypt, balloon, bcrypt and, to a lesser extent, PBKDF2*".

In the present case, the delegation was informed that the passwords of the users of the "[redacted]" game are stored with the SHA-512 hash function.

In the event of a data breach, the use of that algorithm would enable an attacker to search very quickly for the password corresponding to each footprint retained by the company, leading to an increased risk of undermining the confidentiality of users' data.

Therefore, the storage of passwords from the [redacted] accounts is not in line with the state of the art on the day of this Decision since your company does not use a proven and recommended algorithm for hashing passwords.

Therefore, I consider that the company [redacted] infringed the provisions of Article 32 of the GDPR.

---

[2] See Resolution No 2022-100 of 21 July 2022 adopting a recommendation on passwords and other shared secrets

[3] https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

4. On the breach of the obligation to inform the data subjects and obtain their prior consent before registering information on their electronic communications terminal equipment or accessing it (cookies and other trackers)

In law, Article 82 of the French Data Protection Act provides that "*Any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he/she has been informed in advance, by the controller or its representative, of:*

1° The purpose of any action to access, by electronic transmission, information already stored in his/her electronic communications terminal equipment, or to write information into that equipment;
2° The means available to him/her to oppose such action.

Such access or registration may only take place if the subscriber or user has expressed, after receiving this information, his/her consent, which may result from the appropriate settings of his/her connection device or any other device under his/her control."

These provisions shall not apply if access to information stored in the user's terminal equipment or recording of information in the user's terminal equipment:
1° either has the exclusive purpose of enabling or facilitating communication by electronic means;
2° Either, it is strictly necessary for the provision of an online communication service at the express request of the user".

Article 4(11) of the GDPR defines *"consent" as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

In its Resolution No 2020-091 of 17 September 2020 adopting guidelines on reading and writing actions in a user's terminal, the CNIL considers that "*the expression of the user's refusal must not require any action on his part or be capable of resulting in action of the same degree of simplicity as that which makes it possible to express his consent*".

In the first place, the delegation noted, upon arrival on the homepage of the website "[redacted]" and on the website "[redacted]", the presence of an information banner which states that "*cookies allow us to customise content and ads, offer social media functionalities and analyse our traffic* [...]" followed by a link "*Know more*" and a "*Understood!*" button.

The delegation also noted during the access to the [redacted]" website and prior to any action that nine cookies were deposited in the terminal used to perform the control, including the "welcomeVersion" cookie and the cookies relating to the Google Analytics tool.

In this regard, in your reply to the control questionnaire, you state that "*the cookie 'welcomeVersion' (1 or 2, generated randomly) is linked to abtesting that was created several years ago and is probably intended to display a different tutorial depending on the abtesting group, this cookie is no longer used in the game and has no impact on the user*" and that "*the cookies __utma, __utmc, __utmz, __utmt, __utmb are used by Google Analytics, the data from Google Analytics are no longer available on our side, as Google Analytics has not been updated for a long time*".

First of all, I note that the cookie information banner does not comply with the minimum requirements for obtaining prior consent in accordance with Article 82 of the French Data Protection Act, in that it does not

contain a button enabling the user to refuse, easily and by clicking only once, the deposit of cookies. Furthermore, I note that cookies which no longer serve any purpose are still written on your website's visitors' terminal.

In any event, cookies of the Google Analytics solution cannot benefit from an exemption from the requirement of Article 82(2) of the French Data Protection Act. Those cookies are not indispensable for the provision of an online communication service at the express request of the user and, because of their inclusion in the targeted advertising system implemented by Google, they combine that purpose, at least, with that of measuring audience on the company's website. Therefore, their writing is subject to the prior consent of the users.

In the second place, after the creation of an account on the website "[redacted]" and after following the tutorial of the [redacted] game, the delegation noticed the display of another emerging window relating to consent management which specifies "Manage your preferences" and "Authorise".

During the online investigation, the delegation noted that in order not to consent to the processing mentioned by the emerging window, the user must click on the "Manage your preferences" button and then, in a second window, interact with a second button.

This shows that a user who wishes to consent to reading and writing actions does so in one click from the first window, while a person who does not wish to consent has to interact twice with the consent management interface. This makes it more complex for a person to refuse rather than consent to reading and writing actions. The consent obtained by the company [redacted] within the emerging window cannot therefore be regarded as free within the meaning of the abovementioned provisions as clarified by the CNIL guidelines.

The delegation also noted that the same marker window is displayed in the Android and iOS mobile apps "[redacted]" and "[redacted]". Therefore, the consent obtained from these applications is also not free.

In the third place, during the investigations carried out on the website [redacted]", the delegation interacted with the emerging window to refuse further reading and writing actions on its terminal. However, it identified two new cookies placed on its terminal following its browsing on the website. It has been stated that these cookies are linked to the display of advertising.

However, because of their advertising purposes, those cookies do not benefit from an exemption and the collection of individuals' consent, which is therefore necessary, is not collected.

Lastly, it is apparent from the network flow record files captured during the online investigation that, when using the '[redacted] Android application, data such as identifiers, including the unique identifier of the mobile phone used, and its characteristics are recorded or transmitted to third parties, as soon as the application is opened and throughout its use.

It appears from the information provided by the company [redacted] that the purposes for which those actions take place require consent to be obtained. Those data are, for example, transmitted to third parties in order to carry out behavioural monitoring and advertising processing.

These writing and reading actions take place before the user's consent is expressed and despite the user's refusal to the use of trackers.

I therefore consider, in the light of all those factors, that the company [redacted] infringed the provisions of Article 82 of the French Data Protection Act.

II. Corrective measures ordered by the CNIL (Article 20 of the Act of 6 January 1978)

In view of all those factors and, in agreement with the other data protection authorities concerned by that processing, in accordance with Article 20 of Law No 78-17 of 6 January 1978, the company [redacted], established at the address indicated above, is ordered to bring processing operations into compliance within three (3) months of notification of this decision and subject to any measures which it could already have adopted:

- implement a retention period policy for inactive users that does not exceed what is necessary for the purposes for which they are collected, in accordance with Article 5(1)(e) GDPR, unless it is justified that they are stored in response to a legal obligation or for evidentiary purposes;

- inform data subjects, in accordance with the provisions of Article 12 of the GDPR, by providing them with transparent and easily accessible information, in particular by referring them directly from the personal data collection forms to the privacy policy via a link in French;

- transform the passwords of users of the '[redacted]' game prior to their storage into a database by means of a specialised, non-reversible and secure cryptographic function incorporating a salt and sufficient time and/or memory parameters;

- with regard to reading and writing actions in users' terminal equipment, unless cookies and other trackers subject to prior consent are not deposited, make available to data subjects a means of refusing them the same degree of simplicity as that intended to accept their use, for example by offering them a refusal button the title of which could be "Refuse all", or by making available to them any other equivalent and unambiguous solution (see on this point paragraphs 32 to 34 of the Recommendation of 17 September 2020) ;

- cease reading and writing actions in users' terminal equipment, in particular the deposit of cookies, as long as the users have not consented to it, unless such operations meet the criteria for exemptions in Article 82 of the French Data Protection Act. In particular, cookies which do not serve any purpose cannot be deposited on users' terminals.

This decision, which does not require a response from you, entails the closure of procedure No 2024-130C. However, this closure is without prejudice to the right reserved by the CNIL to carry out a new verification mission, in order to check that your company has complied with this formal notice on expiry of the time limit.

In the event of a new verification procedure, if your company has not complied with this decision, a Rapporteur will be appointed who may ask the Restricted Committee to impose one of the penalties set forth in Article 20 of the French Data Protection Act.

This decision may be appealed before the Council of State within two months of its notification.

For more information on the formal notice procedure, you can consult the CNIL website at: https://www.cnil.fr/fr/la-procedure-de-mise-en-demeure-0.

The CNIL's departments [redacted] Legal Officer in the Inspections Department [redacted] IT Systems Auditor in the Inspections Department [redacted] are at your disposal for any further information you may require.

Sincerely,

Marie-Laure Denis