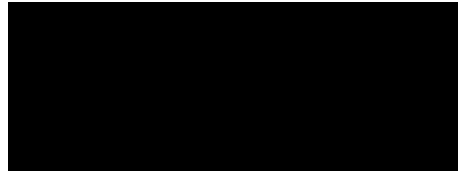


The President



Paris, on July 24, 2024

Our ref.: [REDACTED]

To be stated in all correspondence

Recorded delivery letter N° [REDACTED]

Dear Sir

The main activity of the company [REDACTED] is the sale of wines online in the form of public auctions via its website. It offers its services mainly in France and in several European Union countries. It has nearly [REDACTED] customers accounts in Belgium, nearly [REDACTED] in Germany and nearly [REDACTED] in Italy.

In accordance with **decision No 2023-192C of 26 June 2023**, on 23 August 2023 the Commission Nationale de l'Informatique et des Libertés (CNIL) carried out an online inspection of the website accessible at the URL '[REDACTED]' published by [REDACTED].

The purpose of this inspection was to verify the compliance of the processing implemented by your company with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on data protection (GDPR) and Law No 78-17 of 6 January 1978 as amended. In particular, the purpose of this inspection was to investigate a complaint lodged with the CNIL concerning the use of cookies in the user's terminal before any action being taken when browsing the '[REDACTED]' website, as well as the incomplete and inaccessible nature of the information required by GDPR.

The findings made during this inspection, as well as the additional information provided on 22 September 2023, **lead me to raise the following points.**

I. Analysis of the facts in question

1. Regarding the breach of the obligation to define and comply with a retention period proportionate to the purpose of the processing operation

Article 5(1)(e) GDPR states that personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed [...]*".

In the specific case of the retention of data linked to a user account created on a website, this can in principle be retained until the account is deleted.

— RÉPUBLIQUE FRANÇAISE —

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

1

However, users often stop using these accounts without deleting them, which means that they continue to exist indefinitely. In this case, the principle of limited retention of personal data requires the controller to determine a reasonable period of time after which, if there has been no activity on the part of the user, the account must be considered as inactive and must be deleted, along with the personal data linked to it.

In this respect, the CNIL considers, in its reference framework relating to personal data implemented for the purposes of managing commercial activities,¹ that a period of two years is generally proportionate. It is advisable to warn the users concerned before deleting the accounts of those who have not reacted within the time limit set by the organisation.

In this case, the delegation was informed that data relating to non-customer members is kept indefinitely so that they can access the free services they have requested (access to wine quotations, cellar creation tools, receipt of wine alert emails, etc.). The data is thus retained as long as the member does not delete the account created, regardless of its use. The delegation was informed that this data is not used for commercial purposes.

I therefore consider that [REDACTED] has breached the provisions of Article 5(1)(e) of the GDPR by retaining for an unlimited period the data relating to non-customer members no longer using the services offered by the company.

2. On the breach of the obligation of transparency and to provide information to individuals

In law, Article 12(1) GDPR provides that *“the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language”*.

By way of illustration, the Article 29 Working Party (known as the “G29” and now the European Data Protection Board, EDPB) states, in its guidelines of 11 April 2018 on transparency within the meaning of Regulation (EU) 2016/679, that the criterion *“easily accessible means that the data subject should not have to search for the information but should be able to access it straight away”* and that *“An overriding aspect 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 operation include so as not to be taken by surprise”*. It recommends as a matter of good practice that *“in an online context, a link to the privacy statement or notice should be provided at the point of collection of the personal data, or that this information should be available on the same page where the personal data is collected”*.

The guidelines also state that the information *“should be clearly differentiated from other non-privacy related information such as contractual clauses or general terms of use”*. The guidelines also state that *“the data subject should not have to actively search for the information covered by [Articles 13 and 14] among other information such as the terms of use of a site [...]”*.

¹ https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_traitements-donnees-caractere-personnel_gestion-activites-commerciales.pdf

In this respect, the Commission considers that the information provided to data subjects does not appear on a separate medium from the legal notice and general terms and conditions, but is only accessible via links entitled “General terms and conditions” or “Legal notice”, inserted at the foot of personal data collection forms placed online on a website, and does not enable users to benefit from sufficiently clear and accessible information on the processing of their data. This method of providing information to data subjects does not meet the transparency and accessibility requirements laid down by GDPR. (CNIL, P, 1 December 2021, Formal notice, Company X, No MED-2021-131, unpublished)².

Article 13 GDPR requires the controller to provide the data subject with various items of information, in particular regarding the identity and contact details of the controller, the purposes of the processing carried out, its legal basis, the recipients or categories of recipients of the data, and whether the controller intends to transfer data to a third country. The Regulation also requires that, where it appears necessary to ensure “*fair and transparent processing*” of personal data, that individuals are informed about the period of data retention, the existence of the various rights entitled by individuals, the existence of the right to withdraw consent at any time, and the right to lodge a complaint with a supervisory authority.

In this case, the delegation noted that the creation of a member account is mandatory to buy or sell products on the website “[REDACTED]”. To do so, the user is asked to complete a form, displayed in a pop-up window, including his/her name and email address, and he/she is asked to tick a box to accept the “General Terms and Conditions of Services” (CGS).

The delegation noted that a clickable hyperlink on the term “CGS” sends the internet user to a page that contains several drop-down sections. By clicking on the “Legal notice” section, the user can access the page dedicated to the protection of personal data by clicking on a new very light grey hyperlink.

Furthermore, the delegation noted that said data protection policy contained the majority of the mandatory information set forth in Article 13 GDPR with the exception of that relating to the legal bases of processing and data retention periods.

Finally, following the inspection, the company indicated that it had set up a link on its website entitled “Personal Data”, referring to the page containing the data protection policy, which was not present during the online inspection. Informal checks have confirmed the effectiveness of this change.

It follows from all the foregoing that information relating to the protection of personal data is not easily accessible for users of the website “[REDACTED]” when collecting their data for the creation of an account, as they must actively search for this information among the general terms and conditions of service and carry out multiple actions to be able to access it.

In addition, it appears from the findings made that this information does not specify the legal basis for each processing carried out. Furthermore, information on the data retention period is not mentioned, which in this case does not guarantee fair and transparent processing of individuals’ data.

² See “Table et informatique” (https://www.cnil.fr/sites/cnil/files/202312/tables_informatique_et_libertes.pdf).

I therefore consider that [REDACTED] has breached the provisions of Articles 12 and 13 of GDPR by not providing complete, transparent and easily accessible information to users of the website "[REDACTED]".

3. On the breach of the obligations relating to the joint processing liability

In law, Article 26(1) GDPR provides, in the event of joint processing responsibility, the definition by agreement or in a text of national or Union law of the respective obligations of joint controllers for the purpose of ensuring compliance with GDPR requirements. Article 26(2) requires that the broad outlines of this agreement be communicated to the data subjects.

In this case, the delegation was informed that [REDACTED] and [REDACTED] are jointly responsible for the processing intended to manage buyer and seller customers at auctions. A service agreement dated 3 July 2023 governs the contractual relationship between these two companies. The delegation also noted that the personal data protection policy does not contain any information on the existence of joint responsibility. The general terms and conditions of the services posted online on the "[REDACTED]" website specify the services provided respectively by each of these companies.

However, it appears that the partnership agreement does not define the respective obligations of joint controllers for the purpose of ensuring compliance with GDPR. In addition, no information relating to their respective roles in this processing and their relations with the data subjects is communicated to them.

I therefore consider that [REDACTED] has breached the provisions of Article 26 GDPR.

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 [...]."

Paragraph 3 of this article sets out exceptions to this obligation for operations whose sole purpose is to enable or facilitate communication by electronic means, or which are strictly necessary for the provision of an online communication service at the express request of the user.

Article 4(11) 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 this case, during the online inspection of the “[REDACTED]” website, the delegation noted, when accessing the website and before any action, the deposit of 17 cookies in the browser of the terminal used to carry out the inspection, including Google Analytics, DoubleClick and AdSense cookies. The delegation was informed that the DoubleClick and AdSense cookies have an advertising purpose and that the Google Analytics cookie has an audience measurement purpose. For the latter, it was specified that your company had chosen to no longer use the Google Analytics audience measurement solution.

The delegation also noted, upon arrival on the site’s home page, the presence of an information banner which specified that cookies “allow us to personalise the presentation of our wine selections, according to your preferences and your browsing history” accompanied by two buttons - “I configure my choices” and “I accept” - and a link “I continue without accepting”, located at the top right of the information banner.

Finally, informal findings show that, from now on, eight cookies are placed in the user’s browser as soon as they arrive on the home page and before any action. The DoubleClick, AdSense and Google Analytics cookies are no longer among the cookies placed.

However, in view of all of these factors, I note first of all that cookies not exempt from consent - because they pursue an advertising purpose - were placed on the browser of the users’ terminal without their prior consent.

Then, the cookies of the Google Analytics solution could not benefit from an exemption from the requirement of Article 82(2) of the French Data Protection Act. Indeed, they are not essential for the provision of an online communication service at the express request of the user and, due to their inclusion in the targeted advertising system implemented by Google, they combine this purpose, at least, with that of measuring the audience on the company’s website. Therefore, their storage was subject to the prior consent of the users.

Finally, the information banner relating to cookies does not comply with the minimum requirements allowing the collection of sufficiently informed prior consent and in accordance with Article 82 of the French Data Protection Act in that it does not inform the data subjects of the advertising purpose pursued by the storage of cookies.

I therefore consider that [REDACTED] breached the obligations of Article 82 of the Law of 6 January 1978 as amended.

I also draw your attention to the fact that, in the event that the measurement solution now used by [REDACTED] allows individual monitoring of the user, it could not benefit from the exemptions to consent set forth in Article 82 of the French Data Protection Act. For all practical purposes, I invite you to read the fact sheet published on the CNIL website “Cookies: solutions for audience measurement tools”.³

³ <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-dauidience>

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

Due to all these elements, and in agreement with the other data protection authorities concerned by this processing operation, the following corrective measures should therefore be taken against [REDACTED]

1. **A REMINDER OF LEGAL OBLIGATIONS**, in accordance with the provisions of Article 20.II of the Law of 6 January 1978, with regard to the obligation to obtain consent from individuals to register information on their terminal equipment (cookies) and to access them (Article 82 of the French Data Protection Act).
2. **FORMAL NOTICE** in accordance with the provisions of Article 20.II of the Law of 6 January 1978, within **three (3) months of notification of this decision and subject to any measures it may have already adopted, to:**
 - **define and implement a retention period policy** for data from inactive accounts of non-customer members that does not exceed the period necessary for the purposes for which it was collected, in accordance with Article 5(1)(e) GDPR, unless it is justified in order to meet a legal obligation or for evidential purposes;
 - **inform data subjects**, in accordance with the provisions of Articles 12 and 13 GDPR, by providing them with complete, transparent and easily accessible information, in particular by completing the "Personal Data" policy posted on the [REDACTED] website and by referring them to it from the account creation form;
 - **define the respective obligations of the joint controllers** by means of an agreement and make the outline of this agreement available to the data subjects, in accordance with Article 26 GDPR;
 - **inform individuals of all the purposes pursued by the use of cookies** when browsing the [REDACTED] website, in particular by supplementing the information already present on the "cookies" banner by mentioning the advertising purpose pursued by them.

This decision, which does not require a response from you, entails the closure of procedure No 2023-092C. However, this closure takes place without prejudice to the Commission's right to carry out a new inspection in order to verify that your company has adopted the required measures at the end of the given period.

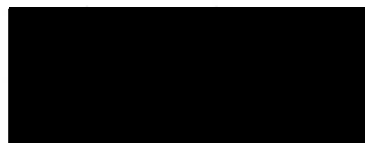
In the event of a new verification procedure, if your company has not complied with this formal notice, a Rapporteur will be appointed who may ask the Restricted Committee to impose one of the penalties set forth in Article 20 of the Law of 6 January 1978.

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] and [REDACTED] Information Systems Auditor in the Inspections
Department ([REDACTED]) are at your disposal for any further information you
may require.

Sincerely

A large black rectangular box redacting the signature of Marie-Laure Denis.

Marie-Laure Denis