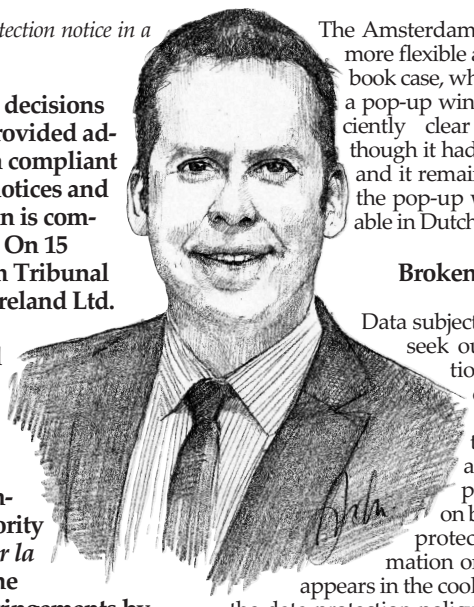
Best practices for drafting and updating data protection notices

How to draft or update a data protection notice in a compliant manner.



Recent administrative decisions and case law have provided additional guidance on compliant privacy or data protection notices and how mandatory information is communicated to data subjects. On 15 March 2023, the Amsterdam Tribunal ruled that Meta Platforms Ireland Ltd. ("Facebook", previously Facebook Ireland Ltd.) had breached its information and transparency obligations, among other things (the "Facebook case")(1). A few months ago, the Luxembourg data protection authority (*Commission nationale pour la protection des données*, or the CNPD) found multiple infringements by several platform providers in Luxembourg during a thematic audit on transparency in the e-commerce business. You may also remember the EDPB decision in the WhatsApp case which had already clarified in 2021 some transparency obligations to which data controllers are subject (*see our article in AGEFI December 2021, p. 43*).

By means of practical examples, we will discuss some best practices for drafting or updating privacy and data protection notices.

Timing and location of the information

Data subjects must receive information on the processing of their personal data when it is most relevant to them, as emphasized by the Amsterdam Tribunal. Transparency increases where the provision of information is spread out in easily digestible chunks and is provided at the time when the personal data is collected for a specific purpose.

For example, in the Facebook case, users were not informed that external developers would have access to their personal data via Facebook when installing an external application. Such information did not appear in the pop-up window, nor was there any link or reference to the privacy policy. Even though Facebook's general privacy policy contained the required information on external developers' access to personal data, and users were made aware of that privacy policy when they first registered for and logged into the Facebook service, such information was at that point in time not considered relevant/not yet at issue for the data subjects. It was therefore, in the opinion of the Amsterdam Tribunal, not the appropriate time to inform them. Facebook had infringed its transparency obligations.

A general reference to a controller's data protection policy will therefore not always suffice. In order to fulfil their legal obligation to inform data subjects, controllers must be able to prove that the information is provided when such information is most relevant for the data subjects.

The CNPD also examined whether users could directly access data protection information without having to take multiple steps, before and after the installation of mobile apps. Where the platform was hosted on a website, the CNPD investigated whether a link to the relevant data protection information was provided at the point of collection of the personal data, or whether this information was directly available on the same page where the personal data was collected.

Languages of the data protection notice

In its thematic audit, the CNPD pointed out that the information must be provided in clear and plain language, which means that the information must be translated in all the languages in which the website and/or mobile app is available. According to the CNPD, the fact that the controller made the website available to users in a certain language B, besides language A, shows that the controller was targeting a public that was not necessarily proficient in language A. The controller could therefore not expect them to understand a data protection policy drafted in language A.

It was of no relevance whether or not language A was the official language of the country. Where the controller operates a website in one or more languages and/or offers specific country options and/or facilitates the payment for goods or services in the currency of a particular country, the controller is deemed to be targeting data subjects in those countries. In such cases, the controller must provide a translation of the data protection information in those languages in order to comply with its transparency obligations.

The Amsterdam Tribunal adopted a more flexible approach in the Facebook case, where it considered that a pop-up window contained sufficiently clear information, even though it had appeared in English and it remained unclear whether the pop-up was also made available in Dutch.

Broken hyperlinks

Data subjects should not have to seek out relevant information on the processing of their personal data. This information must be easily accessible. For example, if there are policies on both cookies and data protection, and the information on personal data only appears in the cookies policy and not in the data protection policy, the CNPD deemed the information not easily accessible for the relevant data subjects.

The same is true where the data protection notice of a controller operating multiple platforms or applications contains confusing information as to which kinds of personal data processing are used for which specific platform of application. Data controllers should also regularly check the validity of the hyperlinks provided on their websites or applications. When the CNPD noted that hyperlinks were broken, and that therefore the data subjects could not easily access the data protection notice, the data controller was deemed to have infringed its transparency obligations.

No anticipation of future processing

It is important that data controllers only include in their data protection notices the processing activities that effectively take place at the time. Although this sounds very logical, the CNPD found more than one instance of information on processing activities that were not taking place at the time of the investigation. Although such processing activities could be envisaged by the controller in the future, data subjects must not be informed of them until such activities actually take place. To be properly understood by data subjects, the notice must reflect the reality of the processing activities effectively in place, and thus without anticipating processing activities that may take place in the future, according to the CNPD.

Furthermore, it goes without saying that the information contained in the data protection notice must at all times be aligned with the information appearing in the controller's record of processing activities. Surprisingly, this point is often overlooked, as evidenced by most of the cases investigated by the CNPD.

Information specific to processing activity and personal data

Information on the legal basis and purposes of the processing, the recipients of the personal data and the retention periods must be provided in such a way that they are linked to the specified processing activity and specified categories of personal data. The EDPB had already made this clarification in the WhatsApp case in 2021. It is not sufficient to provide this kind of information in a general, abstract manner.

Neither can the controller simply state in a general way that personal data will be stored for as long as required for the purpose for which it was collected. The CNPD reminded that different retention periods should be mentioned for the different categories of personal data and/or the different purposes of the processing, including periods for archival purposes.

Recipients of personal data

In principle, the obligation to provide information on the recipients of personal data does not require the provision of a list of all individual recipients; a comprehensible explanation of the categories of recipients is sufficient. That does not, however, prejudice the right of data subjects to request the identity of the individual recipients based on their right of access (see CJEU, C-154/21, RW v. Österreichische Post AG).

In a decision that preceded that CJEU case, the CNPD had held that a data controller that mentioned that an up-to-date list of recipients could be obtained upon a data subject's request was deemed to have infringed its transparency obligation. The CNPD considered such a suggestion as an indication that the information provided was not complete, and thus not clear. In addition, where a list of cookies was indicated as being "non-exhaustive", the CNPD found an infringement due to incomplete information.

Summary of updates

The data controller must notify data subjects of updates to data protection notices in an appropriate way, such as by email, a hard copy letter and/or a pop-up on a webpage. The notification must also be specifically about the changes, which means that the changes must not be communicated together with direct marketing content, for example. The CNPD considered that a cookie banner was not an appropriate means to communicate updates to the data protection notice, and that the notification must also contain an explanation of how the changes could affect the data subjects and a summary of the main changes.

The CNPD took a fairly strict approach. It appeared from the controller's privacy policy that users were not systematically or actively informed in the case of substantial changes to the policy. Even though the investigation showed that the controller had planned to inform users by email of future updates to the privacy policy, the CNPD still considered that the data controller did not provide easily accessible information and had therefore infringed its transparency obligations.

Controllers must understand that references in the privacy statement or notice that data subjects should regularly check the privacy statement/notice for changes or updates are not only considered insufficient but also unfair.

Mandatory fields in online forms

The CNPD specified that online forms must indicate clearly which fields are required and which are optional, and what happens if required fields are left blank. A controller was found to have infringed its information obligations for the processing of online forms because the mandatory fields of the form used to create a personal account on its website were not marked as mandatory when the form was still empty. The mandatory nature of the fields was only indicated when the user attempted to create an account by clicking on the "Register" button without having completed all fields. Furthermore, the data protection notice did not mention the mandatory nature of the information requested in the mandatory fields, nor the consequences for the user if no personal data was provided, even though it was mandatory to provide such data to be able to open a personal account on the website.

Shortcomings of the service provider or data recipients

The controller remains responsible for the lack of a compliant data protection notice even if, in practice, such non-compliance is due to an omission or fault of one of the controller's service providers, for example in a situation where the website operator has refused multiple requests by the controller to include a data protection notice on each interactive web page. On the other hand, the controller will not be responsible for the further processing of personal data by third-party recipients for which the controller does not determine the means and purposes. For example, the Amsterdam Tribunal did not hold Facebook responsible for the further processing of personal data by so-called integration partners after Facebook had shared the data with them, and considered such processing outside the scope of Facebook's information obligations.

Procedure before the CNPD

The recent CNPD decisions concerned a thematic audit on transparency in the e-commerce business. Typically, in the published cases, the CNPD decided to open an investigation, upon which the head of investigation sent the respective data controllers a preliminary questionnaire and then performed an on-site visit. Since it can be important for data controllers to make themselves heard, this could be done on several occasions throughout the procedure: in the questionnaire and the on-site visit, in exchanges between the CNPD's investigation team after the on-site visit, by replying to the statement of objects issued by the head of investigation and finally orally during the administrative hearing before the CNPD.

The CNPD imposed administrative fines ranging from EUR 700 to 3,000, which were in all cases lower than the fines proposed by the head of investigation. Where controllers had already undertaken certain corrective actions with a view to greater compliance of their data protection notices, the CNPD took such actions into account in the assessment of the sanctions, although the controllers were still deemed in breach of the GDPR, based on the situation at the beginning of the investigation. The CNPD also took into account the controllers' cooperative behaviour during the investigative procedure. In most cases, the CNPD also imposed corrective measures to be put in place by the controller within two months.

Conclusion

Although the fines imposed were not significant, the CNPD's decisions are a clear warning that the drafting and updating of data protection notices must be taken (more) seriously. Data controllers must ensure particularly that their data protection notices are aligned with the records of their processing activities, and must pay attention to the timing of the communication of the information to the relevant data subjects. Controllers that operate websites and mobile apps should furthermore not forget to translate the data protection notices in all the languages in which the websites or apps are available.

** Vincent WELLENS (portrait)*
Admitted Lawyer in Luxembourg and Brussels
Partner, NautaDutilh Avocats Luxembourg
vincent.wellens@nautadutilh.com

Sigrid HEIRBRANT
Admitted Lawyer in Luxembourg and Brussels
Senior Associate, NautaDutilh Avocats Luxembourg
sigrid.heirbrant@nautadutilh.com

1) Please note that the decision of the Amsterdam Tribunal will likely be appealed.