

Data Protection notices after the *WhatsApp* case: what's the message?

A few months ago, the Irish Data Protection Commission imposed an administrative fine of EUR 225 million on WhatsApp Ireland Limited, declaring the company's data protection notice non-compliant with the General Data Protection Regulation (Regulation (No) 2016/679 or the «GDPR»).

Although the decision is mostly cited with reference to the transfer of personal data from WhatsApp to Facebook, many points have more general relevance, specifically as regards the content of data protection notices. In addition, the decision is interesting as it was subject to the consistency mechanism and based on a binding Article 65 decision of the European Data Protection Board (the EDPB), meaning it underwent scrutiny by several national data protection authorities.

This article discusses some practical takeaways from the *WhatsApp* case to be considered when drafting or updating privacy and data protection notices.

A LAYERED APPROACH IN ORDER TO ENHANCE TRANSPARENCY

Transparency is a basic principle of data protection law. Data controllers are obliged to provide the information referred to in Article 13 (for the direct collection of data) and Article 14 (for the indirect collection of data) GDPR in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12).

The information referred to in these articles includes the identity and contact details of the data controller (and the DPO, if applicable), the purposes of and legal bases for the processing, the recipients of the personal data, any intention to transfer personal data as well as the transferring mechanism, the retention period(s), the rights of data subjects, whether the provision of data is a contractual or statutory requirement, and the source from which the personal data originate if not obtained from the data subjects themselves. This information should be communicated to the data subjects in a clear and concise manner so as not to overwhelm them with information they do not understand or that is irrelevant to them. In this respect, it is important to avoid confusing and legalistic language in privacy notices.

In the *WhatsApp* case, the Commission assessed, for each item of information required by Articles 13 and 14 GDPR, *how* and *in which way* it was provided.

In order to balance and comply with the obligations to provide data subjects with sufficient and precise information in a clear and concise manner, a layered approach can be used. The use of hyperlinks is permitted and may facilitate the accessibility and readability of a data protection or privacy notice. However, if multiple hyperlinks are used, it is important to ensure that the information does not become less accessible and that this approach does not give rise to discrepancies or pointless, circuitous routes.

Where users are presented with more detailed information when they click the links provided, there is no problem. However, when the information made available by way of embedded links is similar to that available both in the primary text and other linked texts, a significant risk of confusion and opacity arises.⁽¹⁾ Users should not have to «work hard to actively engage with the original text as well as seek out

the additional texts made available by way of [...] various links».⁽²⁾ Nor should they be left wondering if they have exhausted all available sources of information.⁽³⁾

In any event, the privacy notice must be distinct from other policies and notices and not included in the general terms and conditions.

A GRANULAR APPROACH TO THE PROVISION OF SPECIFIC INFORMATION

Legal basis for and purpose of the processing

In assessing the requirements of Article 13(1)(c) GDPR, the Irish Data Protection Commission took the view that, in order to achieve compliance, the data controller must indicate the legal basis for and purpose of the processing activity in such a way that they are linked to the

- specified processing operation or set of processing operations for which the personal data are intended; and
- specified category(-ies) of personal data.⁽⁴⁾

In other words, it is not sufficient to describe in general terms the purposes of and/or legal bases for the data processing activities. Rather each purpose and legal basis should be linked to a specified processing operation or set of operations and to the specified category(-ies) of personal data concerned.

It is therefore common practice to insert in the privacy notice a table indicating (i) the processing operations, (ii) the purpose(s) of the processing, (iii) the categories of personal data concerned, and (iv) the legal basis relied on for each processing operation.

According to the Commission, this approach is the only one that ensures data subjects are provided with sufficient information so that they can meaningfully exercise their rights and assess whether there are grounds for a complaint.⁽⁵⁾

Legitimate interests

According to the EDPB, the same approach must be followed when assessing the information to be provided under Article 13(1)(d) GDPR, which requires that, when processing is based on a legitimate interest of the controller or a third party, the controller must identify the legitimate interest pursued.

An assessment as to whether WhatsApp had provided sufficient information in this regard formed part of the EDPB's binding decision, as the various data protection authorities involved were unable to reach a consensus.

The EDPB is of the opinion that each legitimate interest pursued must be linked to specific information on the corresponding processing operation and the categories of personal data being processed on that basis. Without this information, data subjects are unable to exercise their rights under the GDPR.⁽⁶⁾

The legitimate interests pursued must furthermore be specified in a sufficiently precise manner. The EDPB considered the references by WhatsApp to the provision of «other business services» and the «interests of businesses and other partners» to help them understand their customers [...] to be insufficiently clear as to which businesses or partners were referred to. In addition, the description of the legitimate interest «to create, provide, support, and maintain innovative Services and features [...]» does not meet the required clarity threshold, according to the EDPB.⁽⁷⁾

It follows that data controllers should avoid generic wording when specifying the legitimate interests pursued.

Compliance with a legal obligation

If the data controller intends to base a processing operation on the ground of «compliance with a legal obligation», the notice should identify the relevant EU or national law giving rise to the obligation.⁽⁸⁾

WhatsApp argued that data controllers do not determine the legal obligations to which they are subject, unlike legitimate interests. The Commission declared this argument irrelevant: «If a data controller processes personal data in pursuit of compliance with a legal obligation, then a data controller is in a position to 'readily identify' and inform the data subjects concerned about the processing and the reason for the processing».⁽⁹⁾ Furthermore, it is important to bear in mind that transparency obligations are ongoing and cannot be complied with on a one-off basis. If the controller becomes subject to a new legal requirement to process personal data, it will have to update its privacy notice accordingly.⁽¹⁰⁾

Categories of recipients

The notice must be «as specific as possible» when it comes to categories of recipients in order to ensure that data subjects are provided with meaningful information. The Commission agrees with the Article 29 Working Party Transparency Guidelines,⁽¹¹⁾ according to which the recipients of personal data should in principle be *named* and if the controller opts to indicate *categories* of recipients, the information should be as specific as possible and include:

- the type of recipient (with a reference to the activities it carries out),
- the sector or industry,
- the sector and sub-sector, and
- the location of the recipient.

Data subjects must furthermore be able to identify which categories of their personal data will be received by the indicated (categories of) recipients and why the data are being transferred. Without this information, the Commission is of the opinion that data subjects are unable to understand the consequences of the transfer and assess whether they wish to exercise one or more of their rights.⁽¹²⁾

International transfers

With regard to international transfers of personal data as well, the information provided must be as specific as possible. This means that the notice must identify the adequacy decision relied on. The Data Protection Commission found that use of the word «may» in WhatsApp's notice was, in the context of possible reliance on adequacy decisions, contrary to the requirement to provide clear and transparent information to data subjects.⁽¹³⁾ Users must be able to identify the specific adequacy decision being relied on so that they can access further information. This implies that the data controller should, in principle, also identify the country to which the data will be transferred.⁽¹⁴⁾

Where an international transfer is based on standard contractual clauses, information on the *specific* standard contractual clauses used must be provided. It is not sufficient to simply include a hyperlink to a generic European Commission webpage.

Finally, the required information should be linked to the specified categories of personal data being transferred.⁽¹⁵⁾

Retention criteria and periods

The Data Protection Commission agrees with the Article 29 Working Party Transparency Guidelines⁽¹⁶⁾ that the retention periods for different categories of

personal data and/or processing purposes should be stipulated. Again, a link is required between the categories of personal data and the retention periods or criteria. A data controller cannot merely state, in general terms, that personal data will be kept «as long as necessary» to fulfil the legitimate purpose of the processing.⁽¹⁷⁾

The retention criteria must furthermore be sufficiently clear to data subjects. Practical examples of how each criterion impacts the retention period may be required.⁽¹⁸⁾

Right to withdraw consent

WhatsApp had included the required information about the right to withdraw consent in the «Your Consent» section, rather than in the section entitled «How You Exercise Your Rights».

The Data Protection Commission found that given the title of the latter section, this is where data subjects would most likely search for information about their rights and therefore information on the right to withdraw consent should have been included in this section.⁽¹⁹⁾

CONCLUSION

When drafting or updating data protection notices, it must be ensured that data subjects are provided with sufficient information so that they can meaningfully exercise their rights and assess whether to lodge a complaint. Furthermore, the data controller must provide this information in a clear and concise manner.

In order to balance and comply with the obligations to provide sufficient and precise information in a clear and concise fashion, more detail in data protection notices is expected so that data subjects know which personal data will be processed, for which purpose or legitimate interest, to which country the data will be transferred and/or to which (categories of) recipients.

To this end, a layered approach is permitted and can facilitate the accessibility of privacy notices, provided data subjects receive more detailed information when they click hyperlinks and the links do not lead to pointless, circuitous routes.

Vincent WELLENS (picture)

Admitted lawyer in Luxembourg and Brussels
Partner NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Sigrid HEIRBRANT

Admitted lawyer in Luxembourg and Brussels
Senior Associate NautaDutilh Avocats Luxembourg S.à r.l.
sigrid.heirbrant@nautadutilh.com

1) Irish Data Protection Commission, *WhatsApp* decision, 20 August 2021, para 336.

2) *Ibid.*, para 337.

3) *Ibid.*

4) *Ibid.*, paras 301-302.

5) *Ibid.*, para 309.

6) EDPB Binding Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, 28 July 2021, paras 57 and 59.

7) *Ibid.*, paras 62-64.

8) Irish Data Protection Commission, *WhatsApp* decision, *op cit.*, para 369.

9) *Ibid.*, para 377.

10) *Ibid.*, para 378.

11) Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679

12) Irish Data Protection Commission, *WhatsApp* decision, *op cit.*, para 428.

13) *Ibid.*, para 437.

14) *Ibid.*, paras 449, 450 and 452.

15) *Ibid.*, para 452.

16) Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679

17) Irish Data Protection Commission, *WhatsApp* decision, *op cit.*, para 468.

18) *Ibid.*, paras 470-471.

19) *Ibid.*, para 491.