GDPR series

Transparency

This article first appeared in
Privacy & Data Protection journal

macfarlanes.com

GDPR series: Transparency

Manish Soni, Senior Counsel & Notary, Macfarlanes LLP, advises on how to comply with the GDPR's transparency obligations (drawing on the Working Party's recent guidance)

As organisations are busily preparing for the General Data Protection Regulation's 'go-live' date in May, one of the more onerous obligations that they will need to bear as a consequence centres on the need for 'transparency'. This article explores the recently published guidance from the Working Party on transparency ('the Guidance', copy at www.pdpjournals.com/docs/887866) and considers practical solutions that controllers may draw from it.

Extension to a key principle under the Directive

It is crucial to appreciate at the outset that there is a subtle, but significant, extension to the first data protection principle of the EU Data Protection Directive (95/46/EC) in the GDPR. Whilst the Directive's stated requirement is that personal data be processed 'fairly and lawfully', the GDPR requires fairness, lawfulness and 'transparency'.

The Guidance points out that the Directive did not incorporate the concept of transparency explicitly within its articles, only alluding to it within its Recitals, specifically by making clear that processing could not be fair unless it was also transparent.

The GDPR takes this requirement and extends it through Article 12, which sets out the transparency obligations. Whilst the text of the GDPR does not define transparency, Recital 39 of the GDPR states: "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent."

The Guidance emphasises that transparency applies at various 'stages' of the data processing lifecycle, in particular:

- on (or before) collection at the start of processing;
- throughout processing, when communicating with data subjects about their rights (the Guidance breaks this into a triple obligation, explained below); and
- at specific breakpoints in processing, such as when there are 'material changes' in processing or when a ['high risk'] data breach occurs.

In contrast to the current approach under the Directive, not only will organisations be expected to provide fair and more granular privacy notices, they will also need to be proactive about transparency throughout all processing activities. This could mean, for example, that if an organisation unnecessarily withholds information about a 'high risk' data breach from data subjects, this would amount to a breach of Article 12 in addition to the data breach communication requirement (under Article 34).

It is also necessary to note that the Guidance intrinsically links the new data protection principle of 'accountability' to the transparency requirement and, as such, organisations need to be able to evidence that processing has taken place in a transparent manner. In the data breach example given here, this would require that the organisation be able to evidence the assessment of privacy risk following the data breach.

Elements of transparency

The Guidance describes in some detail the various 'elements of transparency' within Article 12 which are addressed below:

'Concise, transparent, intelligible and easily accessible' — Communications regarding processing should be clearly differentiated from other, non-privacy related, information within a privacy notice. This means the information cannot be included with other terms and conditions and not tagged onto other communications, and individuals should not have to scroll through large amounts of text to find a particular part of a privacy notice.

For complex processing, controllers will need to go over and above the prescribed information to be provided (under Articles 13 and 14) and separately spell out the most important consequences of processing.

For mobile apps, the information should be made available from an

(Continued on page 12)

(Continued from page 11)

online store prior to download and, once the app is installed, the information should never be more than two clicks away.

To comply with the 'easily accessible' requirement, best practice in an online context would be to provide a link to the privacy notice at the point of collection.

'Clear and plain language' — The Guidance emphasises the need to avoid qualifiers, such as 'may' or 'possible'. Sentences such as 'we may use your personal data to develop new services' would not be acceptable. Instead, the active voice and simple – non-legal – terminology ought to be used. Accurate translations should be provided in all relevant languages where different language groups are targeted.

The Guidance provides examples of unclear phrasing, such as: 'we may use your personal data to develop new services'. This is not sufficiently granular since it does not say what the services are or how they will be developed. Another example is 'we may use your personal data to offer personalised services'. Such wording does not extrapolate on what the 'personalisation process' entails.

Providing information to children — Where a controller targets children for the provision of goods or services, or ought to be aware that they are likely to be utilised by children, notices should be appropriately designed to resonate with children. This will almost certainly mean producing a distinct privacy notice for different age groups, children and adults, where both groups are targeted.

"In practice, satisfying the triple obligation will unlikely be straightforward. In some cases, during the lifecycle of data processing the rights that can be invoked will change depending on the lawful base utilised, on whether the purpose for processing continues and on the right invoked itself."

'In writing or by other means' — The default position is that the provision of information to data subjects should be in writing, including in combination with standardised icons where this adds value. For most organisations, this will continue in an online context, to be a privacy notice.

What must be provided in a privacy notice?

The Schedule to the Guidance includes a useful table that summarises the categories of information that must be provided to a data subject, both where information is obtained directly (Article 13) or indirectly (Article 14), which may be worth keeping at hand as a ready resource.

The GDPR text sets out various information that controllers must provide to individuals at the time personal data are collected. The Guidance elaborates on these requirements. Among the more noteworthy elements, controllers should provide clear contact information to data subjects using different methods of communication.

A controller must also indicate any recipients or categories of recipients with whom the controller will share personal data. The Working Party makes it clear that, as a default position, the controller should provide information on actual, named recipients. Where this default position is departed from, a 'category of recipients' may be provided. However, in this case, the controller must:

- be able to demonstrate why it is fair for it to take this approach; and
- be as specific as possible in the privacy notice about the type of recipient, the industry, sector and sub-sector, and the location of the recipients. The 'default' position in naming recipients may be uncomfortable or impractical for some controllers and some care will be needed in satisfying the requirements in the case that the non-default position is adopted.

A privacy notice should explicitly state all third countries (extra-EEA) to which the controller will transfer personal data. If data transfers are not determined internally via the operation of a privacy framework for example, controllers will need to scrutinise where personal data are being transferred, giving the necessary wide interpretation to the term 'transfer' (e.g. including regular access via remote desktop).

'Legitimate interests' (of the controller) is the most flexible lawful basis for processing personal data, but its use needs to be exercised carefully by controllers. The Guidance provides that when a data controller uses legitimate interests, such interests of the controller should be weighed against the fundamental rights and freedoms of the data subject.

The Working Party considers it best practice where legitimate interests are used to include information from such a 'balancing test' in a privacy notice, which would also assist the controller in demonstrating compliance with its accountability obligation.

Information in a privacy notice should allow a data subject to assess what the retention period will be for specific data/purposes, and (if appropriate) different storage periods should be stipulated for different categories of personal data. It will not be sufficient for a controller to state that it will 'retain personal data for as long as necessary for its legitimate purposes'. A privacy notice must include reference to the various rights of a data subject. In particular, the controller must explicitly bring to the data subject's attention the right to object to processing, and this right must be presented clearly and separately from any other information.

How should a controller communicate a privacy notice to data subjects?

Where a controller has an online presence, the Guidance recommends that the controller provides a privacy notice which is layered. The data subject should have a clear overview of the information available to them and on finding detailed information within the layers of the notice. The Guidance provides that the first layer should always contain information on the processing which has the most impact on the data subject and processing which could surprise the data subject.

The Guidance refers to other methods of communicating privacy notices to data subjects. These include privacy dashboards (which would be accessible from a range of applications) and just-in-time notices (which would provide specific privacy information in context, such as by tooltips, throughout the process of data collection). Where an organisation supplies a range of privacy notices for different services, or utilises various technologies (involving the collection and use of differing quantities of personal data), a privacy dashboard may be a good technology to employ.

Use of visualisation tools and icons and considerations of modality

The communication of information in a privacy notice may also include visualisation tools and icons where appropriate, for example, in the context of dealing with privacy notices for children or to highlight key areas of processing.

In practice, the Guidance recognises that non-standardised icons will not necessarily enhance transparency and passes responsibility for the development of a 'code of icons' to the European Commission as a research initiative.

Controllers will also need to consider the appropriate form for the provision of information, such as for smartphone and IoT (Internet of Things) devices. For example, it may not be possible to easily provide information about privacy in an IoT context due to limited space. However, the use of a machine-readable icon, such as a 'QR code', could be utilised.

Communicating changes to a privacy notice

If a controller makes changes to a privacy notice, for example by processing data for a new purpose, the same principles of transparency apply as with the original privacy notice. The communication should be specifically devoted to the change and not, for example, included with direct marketing content. Additionally, requiring data subjects to regularly check privacy notices for updates is contrary to the principle of fairness.

The exercise of data subjects' rights

The Guidance provides that the requirement for transparency places a triple obligation on controllers in respect of data subjects' rights:

- to provide the requisite information on data subject rights to data subjects;
- to comply with the principle of transparency when communicating with data subjects about their rights under Articles 15-22 (concerning access, rectification, erasure, restriction of processing, data portability, objection and automated decision-making) and Article 34 (data breach communication); and
- to facilitate the exercise of data subjects' rights under Articles 15-22.

In practice, satisfying the triple obligation will unlikely be straightforward. In some cases, during the lifecycle of data processing, the rights that can be invoked will change depending on the lawful base utilised, on whether the purpose for processing continues and on the right invoked itself. For example, the right of access will nearly always (subject to any applicable exemption) be available as long as processing continues. However, the right to erasure applies in limited situations, such as where consent is withdrawn (where this was the legitimising criterion) or the purposes for processing have ceased to exist.

Additionally, controllers will need to gain efficiency in distinguishing between the requirements, such as access and data portability.

Final thoughts

UK-based controllers who have already applied the Information Commissioner's Code for privacy notices will have some advantages in respect of GDPR preparation. However, the ICO Code is primarily based on good practice under the current UK regime. As can be seen, the requirements for transparency under the GDPR will be significantly more onerous to satisfy. In major part, this is a consequence of the requirement for transparency throughout the data processing lifecycle; the need for controllers to be able to demonstrate accountability in relation to the transparency requirements (with greater risks being inherent from a failure to do so); the increased granularity of information that is required; and the requirements in relation to form of information provided by controllers, such as layering, other modalities and the target audience.

In practice, a prudent approach for controllers to comply with the transparency requirements would be to review personal data held (considering the organisation's data inventories, repositories and personal data flows), analyse and record the lawful bases of processing, and undertake a key stakeholder training and awareness campaign on the need for transparency and to review the applicability and handling of data subject rights.

Manish Soni
Macfarlanes LLP
manish.soni@macfarlanes.com