GDPR series: Creating and reviewing data protection policies Part 2 — external-facing policies

Following on from Part 1 which looked at internal-facing policies and procedures, Ann Bevitt, Partner at Cooley (UK) LLP, examines how to meet the GDPR's requirements with regard to external facing privacy policies

All organisations have, or should have, a privacy policy informing their customers, potential customers, users, visitors, suppliers and other third parties whose personal data they collect about how they process those data. Many organisations also have other external-facing policies, for example cookie policies, which tell visitors to their website how they and others use cookies, and wireless acceptable use policies, if they offer guests wireless access. All of these external-facing policies will need to be updated to ensure compliance with the requirements of the EU General Data Protection Regulation 2016/279 ('GDPR'). If organisations do not currently have all of the necessary external-facing policies, they will need to adopt such policies to be able to demonstrate their compliance in accordance with the new principle of accountability introduced by the GDPR.

This article looks at the changes that will need to be made to external-facing policies made available to customers, potential customers, users, visitors, suppliers and other third parties whose personal data are collected. For details of the internal-facing policies and procedures which organisations should make available to employees, please see the previous article 'Creating and Reviewing Data Protection Policies Part 1: Internal-Facing Policies', which appeared on pages 6-8 of Volume 17, Issue 8 of this journal.

Role of the privacy policy

The privacy policy plays a key role in communicating to individuals what personal data are processed, for what purposes, to whom and where they are disclosed and transferred. As noted above, a GDPR-compliant privacy policy will assist organisations in demonstrating their accountability. However, such a policy does much more than that: it satisfies the enhanced notice requirements under the GDPR, and thereby establishes the foundation on which organisations can then seek consent from individuals as both a legal basis for processing, and an adequacy mechanism legitimising transfers of personal data outside of the European Economic Area ('EEA'). Having a GDPR-compliant privacy policy is therefore critical to an organisation achieving GDPR compliance.

Content of a GDPR-compliant privacy policy

Many aspects of a GDPR-compliant privacy policy are the same as, or build on, existing requirements under the Data Protection Directive (95/46/EC). However, there are some new requirements to which organisations will need to pay particular attention. All of the requirements, whether old or new, are summarised below with the relevant references to the GDPR.

Where personal data are not collected from individuals directly, a GDPR-compliant privacy policy must describe the types and/or categories of personal data collected about individuals (Article 14(1)(d)) and the source of those data, including if possible whether they came from publicly accessible sources (Article 14(2)(f)). Such a description is not required where personal data are collected from individuals (presumably because, as those individuals are providing their personal data, they are already aware of the types and/or categories being collected) but it is recommended, in the interests of transparency, that the privacy policy provides all of this information for all individuals in any event.

Regardless of the source of the personal data, a GDPR-compliant privacy policy must explain the purpose(s) for collecting personal data and the legal basis for processing them (Articles 13(1)(c) and 14(1)(c)). If the legal basis for processing the personal data is the legitimate interests of the organisation, the privacy policy must identify those legitimate interests (Articles 13(1)(d) and 14(2)(b)). If the legal basis for processing is a statutory or contractual requirement or the processing is necessary for the purposes of contracting with the organisation, and the personal data are collected directly from an individual, that individual should be informed whether he/she is obliged to provide their personal data and the

(Continued on page 8)

(Continued from page 7)

consequences of not doing so (Articles 13(2)(e)). If the legal basis for processing is consent and the personal data are collected directly from an individual, that individual should also be informed of their right to withdraw consent at any time (Article 13(2)(c)).

A GDPR-compliant privacy policy must also explain whether and when an individual's personal data may be disclosed to third parties and the purpose (s) of such disclosures (Articles 13(1)(e) and 14(1)e)). Accordingly, an organisation will need to list the different types or categories of third parties with whom individuals' personal data may be shared and should consider providing links to the privacy policies of those third parties.

There is also a requirement to inform individuals in what circumstances their personal data will be transferred outside of the EEA and the applicable adequacy mechanism relied upon to legitimise such transfer, for example, consent, the EU model clauses, an organisation's self-certification to the Privacy Shield framework, or the organisation's Binding Corporate Rules (Articles 13(1)(f) and 14(1)(f)). Where organisations, particularly those whose businesses are very dynamic, continue their current practice of referring to worldwide transfers, rather than specifying particular countries, this could be challenged as not being specific enough.

GDPR-compliant privacy policies must also inform individuals of their rights to request access, rectification and erasure of their personal data; to restrict processing of their personal data; and of their right to transfer their data to another person (data portability). Individuals should also be informed of their right to complain to a supervisory authority (Articles 13(2)(d) and 14(2)). As a matter of good practice, details of the procedures which individuals need to follow to exercise their rights should also be provided. These can either be contained in the privacy policy itself or in separate policies with links provided in the privacy policy.

> ***"For mobile apps, providing a link to the privacy policy from the app's app store listing, so that it is accessible prior to downloading and installing the app, is recommended. Organisations should also provide a link within the app, for example when accessing the app's settings."***

Organisations must outline in their privacy policies the data retention periods (or policies used to determine such periods) that typically apply to each of the categories of personal data collected (Articles 13(2)(a) and 14(2)(a)). Also, if an organisation uses automated decision-making tools, including profiling, it must provide 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing' for the affected individual (Articles 13(2)(f) and 14(2)(g)). Finally, organisations must identify, and provide contact information for, the controller, and the controller's representative and Data Protection Officer, if applicable (Articles 13(1)(a) and (b), and Articles 14(1)(a) and (b)).

Practical tips on drafting a GDPR-compliant privacy policy

As well as incorporating the provisions outlined above, the GDPR requires organisations to have privacy policies written in clear, plain English (and other languages in which the organisation conducts business) and which are easily distinguishable from other information (e.g. Terms of Service). Transparency requirements are central to the GDPR and organisations should ensure that their privacy policies are very open about how they use individuals' information.

There are a number of other steps an organisation can take to comply with these transparency requirements. These include displaying the privacy policy prominently on its website/online service and ensuring it is clearly labelled and placed in an easily accessible location such as the homepage. Organisations may also want to make the privacy policy conspicuous, for example by using larger type and/or contrasting colour. Formatting the privacy policy so that it can be printed as a separate document is also recommended.

For mobile apps, providing a link to the privacy policy from the app's app store listing, so that it is accessible prior to downloading and installing the app, is recommended. Organisations should also provide a link within the app, for example when accessing the app's settings.

Clarity of language is also very important. Organisations should use plain, straightforward language and avoid technical or legal jargon (Article 12(1)). The GDPR also specifically mandates the use of standardised icons to help individuals easily find information on specific privacy practice and/or privacy settings (Article 12(7)).

Many organisations already use a layered format highlighting the most important and/or relevant privacy practices in their initially-available privacy policy and allowing individuals to click through for further information on areas of particular interest. There is nothing in the GDPR to prevent organisations continuing with, or adopting, this approach.

Cookie policy

If an organisation collects personal data via cookies or other tracking technologies, in order to comply with the GDPR it must describe the types of personal data collected in this way and the purpose(s) for using

the cookies. This information is most easily conveyed by dividing the cookies used into various categories (essential, functional, analytics/ performance, targeted/advertising and social media) and for each category explaining the purpose for which the cookie(s) are used, where an individual can find out more information about the type of cookie(s), and how an individual can prevent the use of certain types of cookies. This information can either be provided in the privacy policy or in a separate cookie policy. If following the layered approach referred to above, organisations could provide some information about cookies in their privacy policies and then allows individuals who want more information to click through to a separate and more detailed cookie policy.

As with their privacy policies, organisations will need to provide conspicuous and accessible information about cookies on their websites.

Other policies

Organisations may have other policies which could need updating in line with GDPR requirements. For example, if an organisation provides Wi-Fi access for individuals, then it should have in place an acceptable use policy, outlining appropriate uses of the organisation's network by individuals and requiring individuals to indemnify the organisation for losses or damages relating to an individual's inappropriate usage. Such a policy will need updating if individuals' personal data are captured as part of their use of the network.

Ann Bevitt
Cooley LLP
abevitt@cooley.com