GDPR in Context: Transparency Requirements – Privacy Statements

Background

The General Data Protection GDPR (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

Overview

In order for processing of personal data to be fair and lawful, it must be transparent. In practice, for most business, this means setting out the "*how, why, where and what*" of its processing activities in a privacy statement.

The GDPR will result in changes to how privacy statements should be presented and what they need to include. The key new requirements under the GDPR are summarised below.

Legal basis of processing

Under the GDPR, privacy statements must clearly state the legal basis for the organisation's processing activities, be that consent, contractual necessity, compliance with a legal obligation, etc. For some of these legitimate processing grounds, the GDPR imposes additional transparency requirements on controllers.

If the basis for processing is a 'legitimate business interest', the privacy statement must expressly define that interest. This new requirement echoes the GDPR's broader theme of 'privacy by design', in that it will require organisations to consider (and express) the basis of their processing from the outset.

If consent is the basis for the organisation's processing activities, the privacy statement must inform the data subject of their right to withdraw consent at any time. While the right to withdraw consent is not new, the express obligation to publicise it in a privacy statement is. The expectation is that as a result of this 'publicity', data subjects will increasingly exercise their rights to withdraw consent and that this will make relying on consent as a ground for processing increasingly unattractive to controllers.

Data retention periods

Privacy statements must now include the period for which data will be stored, or if this is not possible, the criteria used to determine the retention period must be specified.

How onerous this new obligation will be depends on the organisation in question. For example, if an organisation operates in a regulated industry, it only holds data limited to that industry and there are clear statutorily defined retention periods, then including this information in a concise and intelligible statement should be relatively straightforward. By contrast, an organisation that holds a large amount of personal data for a variety of different reasons may struggle to detail their full data retention policy in a concise and clear manner.

In practice, therefore, the emphasis is likely to be on detailing the criteria used to determine the retention period. Organisations may also consider including a link in their privacy statements to a separate and more detailed data retention policy.

---

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Transparency Requirements - Privacy Statements

Data subject rights

The GDPR requires privacy statements to reference the existence of the data subject's new and extended rights, such as the right of erasure, the right of rectification, the right to restrict processing, the right to object to processing and the right of data portability.

Data subjects must be informed of their avenues of complaint and escalation in the event that their rights are not adequately respected. Therefore, privacy statements must include contact details of the data protection officer ("**DPO**") within the relevant organisation (where a DPO is appointed) and details of data subjects' right to complain to the relevant supervisory authority (in Ireland, the Data Protection Commissioner).

If the personal data being collected is required for statutory or contractual reasons, then the data subject must be informed of the consequences of failure to provide the data.

Where the data controller intends to transfer the personal data outside the EEA, the privacy statement must define the legal basis of the transfer (eg adequacy decision, model clauses, etc), which is another more express disclosure which arises under the GDPR. The statement must reference the safeguards in place with the recipient outside of the EEA, and state the means by which the data subject can access or obtain a copy of these safeguards.

Data collected from other sources

As the law currently stands, data controllers who hold data that is not collected directly from the data subject are only obliged to issue the necessary privacy statement information to data subjects "so far as practicable". In practice, this proviso has made the obligation relatively weak and has led to the obligation only being complied with where it is very straightforward to do so.

The GDPR changes this approach. Following May 2018, unless one of the other exceptions applies, organisations which collect personal data indirectly must issue the privacy statement information to the data subject unless it is impossible to do so or to do so would involve disproportionate effort.

The 'impossibility' exception is a high standard and will rarely be met in practice, and the other exceptions listed in the GDPR are either aimed at protecting researchers or cover specific legal or practical situations.

The 'disproportionate effort' exception is, therefore, the exception which will in practice replace the "so far as practicable" proviso provided for in the existing legislation. This, however, has the potential to constitute a material change, as the effort to make the information available to the data subject will need to be disproportionate to the harm cause to his / her privacy rights by not making them aware of the processing. As the harm caused potentially includes the very fact that the data subject will not be aware of the processing and therefore cannot exercise any of his / her rights under the GDPR, it is open to supervisory authorities to take the view that that the effort involved would need to be significant and material in order to be disproportionate to such harm.

For these reasons, and given the enhanced themes of accountability and enforcement in the GDPR, it is expected that regulators will take a narrow view of the 'disproportionate effort' exception.

Transparency Requirements - Privacy Statements

Transparency and the privacy statement paradox

The 'privacy statement paradox' arises due to the fact that, while privacy statements are meant to increase transparency by telling the data subject what an organisation is doing with his / her data, this information is almost hidden away in privacy statements, largely because the vast majority of people do not read them, and instead hurriedly scroll through the terms and conditions of a new app to find the accept button without reading the privacy statement.

The main reason people do not read privacy statements is due to their length and complexity. Recognising this, the GDPR requires organisations to present privacy statements in a "*clear, transparent, intelligible and easily accessible form... using clear and plain language*". However, the GDPR then goes on to require that significantly more detail is included in privacy statements. The GDPR therefore wants privacy statements to be concise, but more detailed; longer, but shorter – arguably (and ironically), creating a new paradox with which businesses will need to grapple.

Resolving the paradox

In the absence of detailed guidance, organisations will need to come up with creative ways of distilling and presenting relevant and mandatory privacy information.

The recitals to the GDPR refer to the potential use of standardised icons in order to give an "*easily intelligible and meaningful overview of the intended processing*". Such icons could be particularly relevant where the information is being made available to children.

Another option is to use 'just-in-time' privacy statements. This means that instead of having one long-form privacy statement which covers all potential uses of a good or service and making it available at the start of an organisation's relationship with the customer, the organisation instead uses multiple, shorter privacy statements which are tailored for the data subjects specific use of a good or service. For example, when using an app, the user may decide to start using the geolocation location functionality (which they had not previously used). Only at this stage is he / she presented with the relevant privacy statement information relating to geolocation data.

Next steps

The first step for any organisation is to map out its organisation processes through the data lifecycle (meaning the collection, use, disclosure, retention and deletion of data). The results of this data mapping process should then be codified into a privacy statement.

Organisations should consider whether they hold data collected from sources other than the data subject. If an organisation collects data in this manner, it will need to apply the new 'disproportionate effort' test in determining the need to publish privacy statements (unless one of the other exceptions applies).

Organisations also need to think about the 'privacy statement paradox' and consider if resolving it presents an opportunity for the business to build customer engagement and trust.

Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com