Client Update

Draft GDPR Transparency Guidelines Issued: What Does Your Privacy Policy Need to Contain?

Late last year, the Article 29 Working Party (the "Working Party") issued detailed draft guidance (the "Guidelines") on transparency under the EU General Data Protection Regulation (the "GDPR"), which comes into force in May 2018. These Guidelines, which will be finalized following a consultation process, contain the Working Party's interpretation of the mandatory transparency information that must be provided to a data subject by way of privacy policy or other disclosures.

One of the express requirements of the GDPR relates to how businesses communicate their use of a data subject's personal information to that data subject at the point of data collection or consent, typically via a privacy policy or notice. Getting this right is crucial. Businesses will need to closely examine their current privacy policies and other disclosures, and consider whether these need revising not just in the light of the GDPR, but also to factor in the requirements listed in the Guidelines, which elaborate on existing GDPR provisions. While the Guidelines will not be binding, data protection authorities may take a dim view of businesses which fail to comply with the Guidelines without good reason, given that representatives from all of the EU data protection authorities are part of the Working Party. Businesses that fail to comply with the information duties under the GDPR will face fines of up to the higher of 4% of annual worldwide turnover or EUR 20 million.

THE WORKING PARTY GUIDELINES

First, what information must businesses include in their privacy polices?

- *Identity and contact information for the controller/data protection officer* (where applicable[1]): this allows the data subject to easily identify who the controller is and should, where possible and practicable, include several methods by which the controller can be contacted (*e.g.* phone number, email address, postal address).

[1] The Working Party has prepared specific guidance on Data Protection Officers (WP 243, last revised and adopted on 5 April 2017).

- *Purposes and legal basis for processing*: companies should include the legal basis relied upon for processing alongside the purposes for which the data is processed. The Guidelines do not specify whether the privacy policy must list the legal basis for each category of data processed (e.g., names, telephone numbers, e-mail addresses).
- *Legitimate interests*: where legitimate interests are relied on by the controller or third party as the legal basis for processing, the specific legitimate interests need to be expressly stated in a way the data subject can understand. Businesses should also consider, as best practice, providing the data subject with information on how the data controller balances its own interests against those of the data subject. Businesses should carefully consider how to execute this in practice; succinctly summarising the "balancing test" while also ensuring it is easily understandable might seem challenging, but is worthwhile where practicable in order to demonstrate compliance with, for example, the GDPR's accountability principle.
- *Recipients or categories of recipients of personal data, including third parties, joint controllers and processors that receive data*: the default position is that information must be provided on any named recipients. In many cases, for example where the controller engages various data processors, the identity of which may change from the time to time, this task may be onerous and not always practicable. If the controller elects to provide categories of recipients instead of individual names, the controller must be able to show why it did so and provide as much information as possible in the privacy policy, such as information about the type of recipient (by reference to the activities it carries out) and the industry, sector and sub-sector, as well as where the recipients are located.
- *Transfers of data to third countries, along with the safeguards in place and where copies of such safeguards can be found* (*e.g.* via a link): the privacy policy should specify the basis for any data transfer outside the European Economic Area (*i.e.* binding corporate rules, adequacy decision, standard contractual clauses and derogations), along with a list of third countries to which data will be transferred. The Guidelines state that the list must be exhaustive.
- *The retention period*: the Guidelines state that it is insufficient to state, in general terms, that personal data will be held for as long as is necessary for the purposes for which it was processed. Businesses can use statutory requirements or industry guidelines as a means of assessing how long personal data should be kept, but the overarching purpose is to allow a data subject to assess the relevant storage periods, depending on the categories of data provided. Where the data is being held due to an ongoing commercial, business or employment relationship, it may not be possible for the controller to specify an exact retention period, but the data subject should have sufficient information to be able to determine the period.
- *Data subjects' rights*: a privacy policy should include information on how a data subject can access, rectify, erase, restrict processing of, object to the processing of and port their data. These rights must be explicitly brought to the data subject's attention. While stated in the

Guidelines, although not expressly required by the GDPR, this information may need to be accompanied by explanations on what the right involves and how it can be exercised.

- *How a data subject can withdraw consent*: not only does this need to be contained within the information provided to data subjects, but businesses need to ensure that their systems and processes can actually effect the withdrawal of consent as easily as it was given.
- *The right to complain*: data subjects need to be made aware of their right to complain to the relevant supervisory authority in the event of an infringement (actual or alleged) of the GDPR.
- *Use of mandatory fields*: online forms need to indicate clearly which fields are mandatory and which are optional, as well as the consequences of not completing the mandatory fields. For example, in an employment context there may be a contractual requirement to provide certain information to an employer.

Second, the GDPR requires businesses to provide information to data subjects in a way that is "concise, transparent, intelligible and easily accessible". What does this mean for privacy policies in practice?

- Information on the processing of a data subject's personal data must be presented in an efficient and succinct manner, in order to avoid "information fatigue". Using layered privacy statements is a good way of ensuring a privacy policy is easily navigable and user-friendly. Alternative means available to online businesses include "just-in-time" contextual pop-up notices, 3D touch or hover-over notices and privacy dashboards.
- Businesses can make their privacy policies easily and readily accessible by making the information available on the same page on which personal data is collected and by clearly signposting it. The Guidelines consider that combining a privacy policy with other terms and conditions or only providing a link to the privacy policy on the first page of the website will be insufficient.
- The privacy policy must be easy to understand. Businesses should establish who their intended audience(s) are and what the average member's level of understanding may be, taking particular care where their goods/services target children or vulnerable members of society. User panels can be used to test whether an intended audience understands the privacy policy relevant to the processing of their personal information.

Third, businesses will need to monitor their compliance with the transparency requirement regularly throughout the life cycle of processing (for example when data breaches occur) and not only at the point when data is collected from the data subject or otherwise obtained.

Fourth, complying with the current draft Guidelines does not necessarily ensure future compliance. The Working Party will publish updated Guidelines along with a *FAQ* section once it has analysed the responses to its transparency consultation, and the UK Information

Commissioner's Office will continue to revisit its approach as future EU guidelines and best practices develop post-May 2018. Businesses should do the same to ensure they meet the regulators' evolving expectations as the GDPR comes into force and is enforced.

Debevoise advises businesses, both in and outside of the European Union, on all aspects of GDPR preparedness.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

FRANKFURT

Dr. Thomas Schürrle
tschuerrle@debevoise.com

Dr. Friedrich Popp
fpopp@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com

Ceri Chave
cchave@debevoise.com

Christopher Garrett
cgarrett@debevoise.com