

You Want *What?*: Responding to Individual Requests Under the GDPR

July 18, 2018

With the EU General Data Protection Regulation (“GDPR”) in force for less than two months, many companies are already experiencing an increase in requests from individuals seeking to obtain a copy, or request correction or erasure, of their personal data under Articles 15 to 17 of the GDPR.

**Debevoise
& Plimpton**

Do we have to respond? Yes. A response is required even if the response is that the company will not honour the request because a relevant exemption applies.

Can we ask for additional information? Yes. If you have any doubt that the requester is who he/she claims to be, ask for information necessary to ascertain the requester’s identity or to confirm how the requester has interacted with your company in the past. Where appropriate, you can also ask the requester to limit the scope of the request or otherwise engage with him/her to understand the “root cause” of the request. Individual rights requests are rarely made in a vacuum and usually form part of a wider context—for example, a customer service complaint or an employment dispute. Understanding that context may help narrow the request or eliminate it altogether.

How quickly do we have to respond? The standard response period under the GDPR is one month from receipt. That can be extended by two months where necessary, taking into account the complexity and number of requests. Where possible, it is best to keep to the one-month response period. In our experience, extending the response time is likely to lead to an expectation on the requester’s part that the request would be fully honoured and, where the request is for a copy of personal data, an expectation that significant amounts of data would be produced.

Do we need a form, policy, or procedure for individual requests? GDPR does not require these, but it makes good sense to have them if you expect to receive numerous requests. An internal policy or checklist setting out the process can help ensure consistent, GDPR-compliant responses. Conversely, there is no requirement that the requester use a specific procedure or form to submit a request. Nor is there any obligation on you to have an online form available for that purpose. Deciding whether

to publish such a form requires balancing cost and benefit. Responses submitted via a publicly available form may be clearer, but you may get more of them.

When can we refuse to comply with a request, in whole or in part? Unfortunately, this question does not lend itself to a short answer. The GDPR sets out a number of exceptions and limitations on individual rights requests, as does EU Member State domestic legislation (this being one of the few areas under GDPR where Member States have some discretion to set their own rules). These may include circumstances where personal information of other individuals would have to be disclosed, where the request is manifestly unfounded or excessive, or where compliance would compromise your compelling interests or public interest, among others. Careful consideration needs to be given to these factors to determine the best basis, if one exists, to object to a particular request.

Jeremy Feigelson
Partner, New York
+1 212 909 6230
jfeigelson@debevoise.com

Jane Shvets
Partner, London
+44 20 7786 9163
jshvets@debevoise.com

Christopher Garrett
Associate, London
+44 20 7786 9072
cgarrett@debevoise.com