

Right to be Forgotten



“Promise me you’ll never forget me, because if I thought you would, I’d never leave”

Winnie the Pooh, Intellectual thought-leader

Article 17 of the General Data Protection Regulation sets out a right to erasure, also known as a “right to be forgotten” as being:

“the right to obtain from the data controller the erasure of personal data concerning him... without undue delay”

where one of four grounds applies: (i) the data are no longer necessary for the purpose collected or processed; (ii) the data subject withdraws consent and no legal grounds for processing remains; (iii) the data subject objects to the processing; or, (iv) the processing does not otherwise comply with the GDPR.

Article 17 states that the right is particularly significant in relation to personal data made available while a data subject is a child.

What does it involve?

In practice, this means that such data would have to be deleted entirely from the controller’s system and, if the controller has made the information public (such as on the internet), the controller would have to ensure the erasure of links to the information.

Disabling a person’s social media profile or otherwise hiding it from view will not be enough and the requirement is clearly one

of “erasure”. This issue and the right to data portability are likely to trigger wholesale changes in the way that many controllers handle data.

The proper implementation of a framework through which a controller can mobilise such a request is likely to represent a significant burden. Many online services hold vast amounts of personal data and the issues that they will face are clear, in terms of the potential number of requests that they may face and the mechanics of how to quickly and efficiently effect such a request.

Current position

The Court of Justice of the European Union has stated in the May 2014 case of *Google Spain –v- Mario Costeja González*, the CJEU emphasised that the existing Data Protection Directive already included a “right to object” which provides that a data subject can “object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him”. The right to object contained in the Directive had been transposed by Member States in an inconsistent manner, although the *González* case has gone some way to confirming the position.

Reaction time

There is a requirement to act without delay unless there is a legitimate reason not to do so, such as an argument of freedom of expression or a necessity to keep the data for scientific research or if the rights of another party are protected by retention.

Third parties

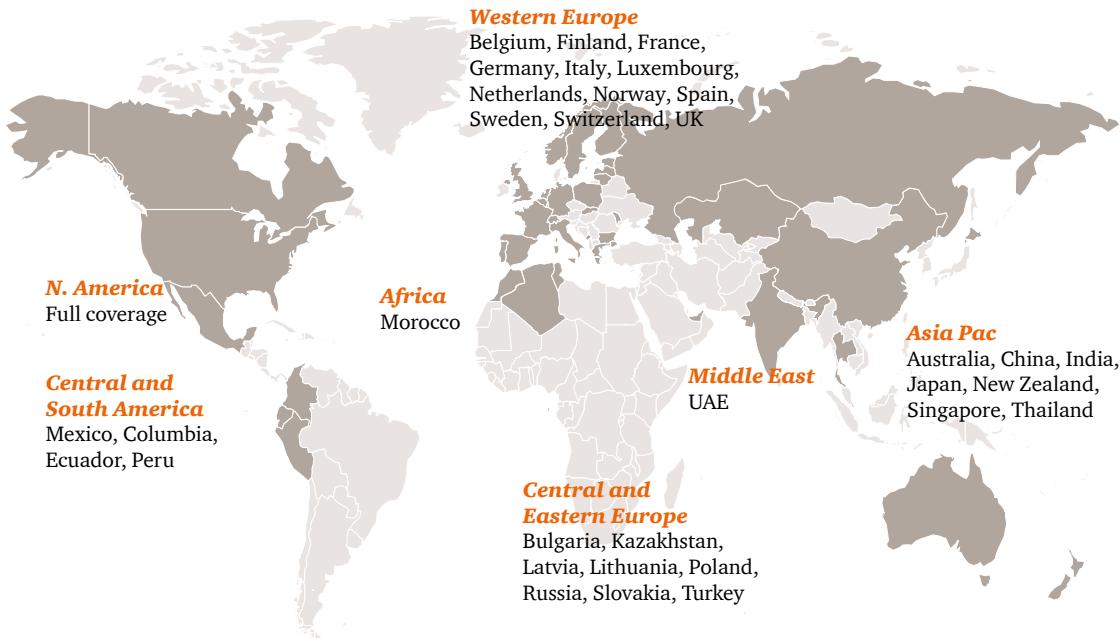
The GDPR now burdens controllers with the responsibility for the removal of content held by third parties.

Recital 54 to the Regulation confirms the position set out in Article 17(2a) and that “a controller who has made the personal data public should be obliged to inform the controllers which are processing such data to erase any links to, or copies or replications of that personal data”. This is likely to be an onerous burden for, in particular, those in the online environment, and will, for example, enable third parties such as publishers to have almost a right of response when requests are submitted to search engines in respect of their content.

Political hot topic

This is a political “hot topic” and has been one of the most discussed aspects of the GDPR and this is an area that has met with some opposition – not least from online service providers and social networks – on the basis that it is a threat to business models that rely on the commercial exploitation of personal data. This right is also viewed as somewhat inconsistent with freedom of expression and is seen as a tool with which people may seek to escape their past.

PwC's global privacy practice



PwC Luxembourg Contacts



Vincent Villers

Partner
2367
vincent.villers@lu.pwc.com



Frédéric Vonner

Partner
4173
frederic.vonner@lu.pwc.com



Sami El Euch

Director
2685
sami.eleuch@lu.pwc.com



Cédric Nédélec

Data Protection Officer
2186
cedric.nedelec@lu.pwc.com

Document version 2. This publication has been prepared by PricewaterhouseCoopers Legal LPP (1, Embarkment Place, London, UK, WC2N 6RH) for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Legal LLP (London), its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers Legal LLP (London). All rights reserved. PricewaterhouseCoopers Legal LLP (London) is a member of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.