GDPR series: the Right to be Forgotten

Hugh McCarthy, Associate with Arthur Cox, examines the GDPR's right to be forgotten and considers the exceptions to this data subject right

Of the various data subject rights under the General Data Protection Regulation ('GDPR'), the so-called right to be forgotten ('RTBF') perhaps attracts most attention. When considering the RTBF, it is important to remember that this right is only available to data subjects in certain circumstances and its application is subject to the various exceptions examined below.

Google Spain v Gonzalez

The RTBF came to particular prominence due to the Court of Justice of the European Union's ('CJEU') landmark 2014 ruling in *Google Spain v Gonzalez*. Based on the premise that Google's search engine activities (of indexing, storing and making information available to the public) constituted 'processing of personal data' under the Data Protection Directive (Directive 95/46/EC), and consequently that Google was a data controller, the CJEU ruled that Google was required to permanently erase links from its search results relating to the plaintiff. The Court established that this right was available not only where search results are inaccurate, but also where they are 'inadequate… no longer relevant or excessive in light of the time that has elapsed'. In terms of precedent, the Gonzalez ruling is limited to search engine results and the underlying news articles containing the relevant personal data were unaffected.

Article 17 of the GDPR

By contrast, the RTBF under Article 17 of the GDPR provides data subjects with a more general right to request erasure of personal data relating to them and in a wider set of circumstances. Subject to the exceptions discussed below, controllers are required to erase personal data (within one month of receipt of a request) in the following circumstances:

- where personal data are no longer necessary for the purposes for which they are processed;
- where the data subject withdraws their consent (and the processing is based on consent);
- where the data subject objects to legitimate interest-based processing (and the controller does not have an overriding legitimate interest);
- where the personal data have been unlawfully processed;
- where EU or national law requires erasure of the personal data; and/or
- where personal data have been collected in relation to a service offering by an information society service offered to children (i.e. data subjects under the age of 13 or 16 depending on the Member State).

The RTBF is not an absolute right and controllers should carefully consider the various exceptions to the RTBF when responding to any data subject requests.

The exceptions to the RTBF may be generally categorised as exceptions based on: (i) lawful basis; (ii) freedom of expression; (iii) other potential exemption; and (iv) limitation on the territorial scope of the RTBF.

Category 1 — Exceptions based on lawful basis

Exemptions to the RTBF apply where processing is supported by certain of the lawful bases under Article 6 GDPR. In particular, the RTBF is not available to data subjects where the processing is:

- necessary for compliance with an obligation under EU or Member State law, or for the performance of a task carried out in the public interest, or in the exercise of an official authority by the controller (as supported by EU or Member State law) subject to the data subject's right to object. Much of public body data processing is supported by these two lawful bases, and as a practical consequence the RTBF may not be available in respect of a portion of public sector data processing;
- necessary for the establishment, exercise or defence of legal claims. This basis is closely linked to the controller's obvious and justified interest in retaining personal data to the extent that it is relevant to legal proceedings;
- based on the legitimate interests of the controller (or a third party) and, notwithstanding the data subject's objection under Article 21 of the GDPR, the controller can demon-

(Continued on page 16)

(Continued from page 15)

strate 'compelling legitimate grounds that override' the data subject's objection (with one example being where processing is necessary for the establishment, exercise or defence of legal claims). This analysis necessarily involves a balancing test between the respective interests and rights of the controller and the data subject;

- where the processing is necessary for archiving purposes in the public interest, scientific or historical or statistical purposes in line with the technical and organisational measures specified in Article 89. This exception is applicable only to the extent that exercise of the RTBF is likely 'to render impossible or seriously impair the achievement of the objectives of that processing'. In short, the data subject's RTBF must be balanced against certain other objectives which justify retention of the data; and
- where the processing is necessary for reasons of public interest in the area of public health. This exception is limited to certain data processing in the public health sphere.

In light of the above exemptions, controllers that clearly map and document the lawful bases supporting their data processing operations will be in a strong position to assess RTBF requests (and other data subject requests), and to identify which, if any, of the above exceptions might apply.

> ***"A potentially more cost-effective alternative to deleting personal data in response to multiple RTBF requests is to irreversibly anonymise the relevant dataset, such that the data no longer constitutes 'personal data'. Of course, this approach will not be practical in all cases, but it is worth considering as a viable alternative to erasing personal data."***

Category 2 — Freedom of expression and information

The RTBF shall not apply where the relevant data processing is necessary for the exercise of the right to freedom or expression ('FOE') and information. This vague statement contained in Article 17(3)(a) must be read in tandem with Article 85 of the GDPR, which requires each Member State to strike a balance between FOE and data protection through their own national law. Indeed, Article 85(1) imposes a positive legislative obligation on individual Member States to 'reconcile the right to protection of personal data...with the right to freedom of expression and information, including processing for journalistic purposes'. In doing so, Member States are guided by Recital 153, which asserts that 'it is necessary to interpret notions in relation to freedom of expression, such as journalism, broadly'.

Article 85 also identifies those areas of the GDPR in which Member States may derogate based on FOE grounds – these include: (i) the Article 5 principles; (ii) the lawful bases under Article 6; (iii) restrictions on data transfers; and importantly (iv) the data subject rights contained in Articles 12 to 21 of the GDPR.

However, Article 85(2) permits derogations on FOE grounds only to the extent necessary to reconcile the right to data protection with FOE or freedom of information. It is expected that national legislatures will introduce general provisions that largely mirror Article 85 in their national law, leaving domestic courts to articulate the contours of the FOE-based exemption on case-by-case basis. Of course, this legislative approach is an invitation for divergence across Member States and flies in the face of the GDPR's purported harmonisation of EU data protection law. In any event, depending on the type of provisions crafted by Member States, the FOE exemption is likely to be a future source of data protection litigation.

Category 3 — Other 'potential' exemptions

Manifestly unfounded or excessive requests — Where a RTBF request is 'manifestly unfounded or excessive', Article 12(5) of the GDPR states that a controller may refuse to act on it. However, this language confirms the high threshold to be overcome and the burden of proving the manifestly unfounded or excessive nature of the request rests on the controller. Accordingly, it would appear that this carve-out will likely be limited to exceptional cases, and will not represent a viable option for refusing RTBF requests in the majority of cases.

Household exemption — Another alternative worth brief mention is the so-called 'household exemption', which places data processing that takes place 'in the course of a purely personal or household activity' outside the GDPR's scope. Examples offered in Recital 18 include 'correspondence and the holding of addresses, social networking and online activity'. However, to meet this description the processing must relate 'a purely personal or household activity' – a term which has been interpreted restrictively under the equivalent clause of the Directive. In short, this will not generally be available to controllers operating in a professional or commercial capacity.

Anonymisation of personal data — A further option open to data controllers is to anonymise personal data. The RTBF is in essence the procedural channel through which individuals can give effect to the principle of data minimisation (under Article 5 of the GDPR). However, data controllers should remember that this principle does not necessarily require deletion of personal data after the relevant purpose has expired. Data minimization in fact prescribes that personal data not be retained 'in a form which permits identification of data subjects' beyond the relevant purpose. Accordingly, a potentially more cost-effective alternative to deleting personal data in response to multiple RTBF requests is to irreversibly anonymise the relevant dataset, such that the data no longer constitute 'personal data'. Of course, this approach will not be practical in all cases, but it is worth considering as a viable alternative to erasing personal data.

E-Commerce Directive safe-harbours — Faced with a claim for breach of Article 17 of the GDPR, the e-Commerce Directive (Directive 2000/31/EC) potentially offers further defences to online controllers. The so-called safe-harbours under Articles 12, 13 and 14 of the e-Commerce Directive insulate providers of 'information society services' (i.e. online platforms) from liability for hosting and transmitting content contingent on two general conditions: (i) that they do not have 'knowledge' of the infringing activity/content; and (ii) they remove the infringing content on receipt of notice. Article 2 of the GDPR provides that the application of the GDPR will be 'without prejudice' to application of the e-Commerce Directive safe-harbours. While the relationship between the e-Commerce Directive and the GDPR is one of mutual ambiguity, for controllers operating in the online space, it may be one worth further exploring.

Category 4 – Territorial scope

Where none of the exemptions above apply and the RTBF is available, the question of its geographic scope is very much a live one. This issue is at the heart of a case that is currently pending before the CJEU, which arose from an enforcement action taken by CNIL, France's data protection regulator, against Google arising from Google's failure to apply the RTBF on a global scale. If implemented, this approach would require Google to delist search results from all of its platforms both within and outside of the EU, including those in the US and elsewhere.

This approach potentially generates tension with the laws of other jurisdictions outside the EU which have a different approach to FOE and the freedom to impart information. For example, any outcome where Europe's highest court compels controllers (for the purposes of EU data protection law) to delete search results accessible in the US, would be very difficult to reconcile with the well-established freedom to impart information under the First Amendment to the US Constitution.

A recent ruling from Canada's Supreme Court has placed it at loggerheads with US courts on this point. In short, it would seem counterintuitive for a law to impose its own singular view on jurisdictions outside the EU, where that law — by design or default — expressly facilitates divergence as between EU Member States' own application of the FOE exemption to the RTBF. The outcome of the CJEU's ruling in *Google Inc. v CNIL* is being closely watched.

Final remarks

While some of the exemptions to the RTBF will seldom be available, and others require clearer elaboration both through domestic legislation and by the courts, controllers should be aware of the scope of both the RTBF and its various exceptions. The young man knows the rules, according to the old adage, but the old man knows the exceptions. When considering the GDPR's right to be forgotten, controllers should be mindful of both.

Hugh McCarthy
Arthur Cox
hugh.mccarthy@arthurcox.com