# Advocate General opines on multiple controllers, consent, the right to erasure and the EU GDPR (Proximus v Gegevensbeschermingsautoriteit)

This analysis was first published on Lexis®PSL on 14 June 2022 and can be found here (subscription required).

**Information Law analysis: This Opinion of Advocate General Collins considers the scope of the obligations under the ePrivacy Directive and the EU's General Data Protection Regulation (EU GDPR) on controllers where multiple controllers in a supply chain process data for the same purposes. While this case concerned public directories, it contains important points for controllers in a wider context. At the heart of these are: (1) controllers must be able to demonstrate any consent they rely on to process personal data and should never simply assume that an individual has given consent; and (2) data subjects are free to approach any controller in a given supply chain to withdraw their consent (or request erasure of their personal data), at which point it is the obligation of the controller so approached to take reasonable steps to inform the other controllers in the supply chain. Written by Marc Dautlich, partner at Bristows LLP and Jamie Cox, associate at Bristows LLP.**

*Proximus NV (Public electronic directories) v Gegevensbeschermingsautoriteit* (Opinion) Case C-129/21, ECLI:EU:C:2022:332

### What are the practical implications of this case?

Advocate Generals present opinions on cases brought before the Court of Justice that raise new points of law. Such opinions are carefully considered by the court but are not legally binding. The Court of Justice often follows the Opinion, but may not do so.

The Opinion considered obligations on operators of public directories under Directive 2002/58/EC (ePrivacy Directive) and Regulation (EU) 2016/679 (EU GDPR). The Opinion has wider applicability, subject of course to the judgment of the Court of Justice, which is awaited. Unless specified otherwise, references to Articles in this summary are references to Articles of the EU GDPR.

The Advocate General firmly takes the view in the Opinion that controllers must take reasonable steps to pass on data subject requests to other controllers in the supply chain processing the same data. Failure to do so can result in all controllers unlawfully processing the personal data. It would follow that controllers should accordingly review:

- all data flows across such supply chains to ensure that they comply with their general obligations of accountability and that their data processing complies with the EU GDPR
- what practical steps they take on receipt of communications withdrawing consents and erasure and rectification requests. Following the Advocate General's assessment that for a data subject to 'withdraw' consent as provided for in Article 12 of Directive 2002/58/EC in this case also encompassed an Article 17 request for erasure, controllers should make sure that, where the data subject is requesting erasure of their personal data, the controller actually erases the data, not merely recategorises it

The Opinion also argues that, unless stated otherwise, a data subject's withdrawal of consent will require the erasure only of the data that is the subject of the specific processing. This was important in this case as Proximus argued that any withdrawal of consent would require both it and Telenet (which collected the original consent and had a separate contractual relationship with the complainant for the provision of telecommunication services) to delete the complainant's record from all their databases, rendering Telenet's contract with the complainant impossible to perform. The Advocate General's view was that this argument is incorrect as the consent related only to the processing of the claimant's data for purposes connected with directories. Upon the complainant withdrawing his consent, Proximus was obliged to remove only the data being processed for purposes connected with the directories, not all data. Otherwise, the complainant would be unable to exercise his right to

withdraw his consent without also having to terminate the wider contract with Telenet, which went against the principle of consent being as easy to withdraw as to give.

**What was the background?**

Proximus provides telecommunications services, including a number of electronic directories containing contact details of both its subscribers and the subscribers of other telecommunications providers. It then offers its lists of contact details to other companies providing directory services. In Proximus' databases, individuals are marked with either 'NNNNN' or 'XXXXX' depending on whether their contact details should, or should not, be included in directories.

The complainant had a contract with Telenet for the provision of telephone services. Telenet shares its subscribers' contact details with a number of third parties, including Proximus.

After seeing his contact details on one of Proximus' directories, the complainant requested his data be removed. Proximus complied with this request by changing the complainant's status to 'XXXXX' in its databases. However, Telenet subsequently sent Proximus an updated subscriber list with the complainant listed as 'NNNNN'. As this indicated that the complainant's details could be included in directories, Proximus automatically re-instated its entry for the complainant in its directory. The complainant discovered that his information was in the directories again and submitted a second request to Proximus, along with a complaint to the Belgian data protection authority.

In the first instance, the Belgian court ruled against Proximus, ordering it to, inter alia, cease the processing and pay a fine of €20,000. Proximus appealed this decision to the Belgian Court of Appeal, which referred four questions to the Court of Justice:

> '(1) Must Article 12(2) of Directive 2002/58, read in conjunction with Article 2(f) thereof and Article 95 of the [EU GDPR] be interpreted as permitting a national supervisory authority to require a subscriber's "consent" within the meaning of the [EU GDPR] as the basis for the publication of the subscriber's personal data in public directories and directory enquiry services, published both by the operator itself and by third-party providers, in the absence of national legislation to the contrary?
>
> (2) Must the right to erasure contained in Article 17 of the [EU GDPR] be interpreted as precluding a national supervisory authority from categorising a request by a subscriber to be removed from public directories and directory enquiry services as a request for erasure within the meaning of Article 17 of the [EU GDPR]?
>
> (3) Must Article 24 and Article 5(2) of the [EU GDPR] be interpreted as precluding a national supervisory authority from concluding from the obligation of accountability laid down therein that the controller must take appropriate technical and organisational measures to inform third-party controllers, namely, the telephone service provider and other providers of directories and directory enquiry services that have received data from that first controller, of the withdrawal of the data subject's consent in accordance with Article 6 in conjunction with Article 7 of the [EU GDPR]?
>
> (4) Must Article 17(2) of the [EU GDPR] be interpreted as precluding a national supervisory authority from ordering a provider of public directories and directory enquiry services which has been requested to cease disclosing data relating to an individual to take reasonable steps to inform search engines of that request for erasure?'

**What did the Advocate General opine?**

The Court of Justice was asked to consider four specific questions related to obtaining and managing a subscriber's consent. After ruling that each question was relevant to the dispute, the Advocate General gave his opinion on each question in turn.

The Advocate General's view was that, based on the wording of Directive 2002/58/EC, consent is required to include a subscriber's contact details in directories. He argued that directory providers cannot assume that a subscriber has consented to their data being processed. Instead, the controller must be able to demonstrate such consent, even if (in the case of directories, as a result of a specific statutory provision to this effect, which was not in contention) it may rely on consent that was originally provided to another controller.

The Opinion suggests that a request from a subscriber to have their data removed from directories constitutes an exercise of the right to erasure under Article 17 of Regulation (EU) 2016/679. Article 12(2) of Directive 2002/58/EC says that subscribers must be able to 'correct or withdraw' their personal data. These words should be given their ordinary meaning, such that 'correct' should mean changing a spelling or address, while 'withdraw' should mean that the controller must cease

processing the data. It follows that any data that is subject to such a request should be deleted, and not just hidden in the controller's database.

Controllers need to take appropriate technical and organisational measures to inform third party controllers that receive the data, of a subscriber's withdrawal of consent. This, in the Advocate General's opinion, is because the general obligations on controllers in Articles 5(2) and 24 of Regulation (EU) 2016/679 require them to take steps to ensure that any data processing complies with the EU GDPR. The Advocate General's view was that, where a controller receives a data subject's request for erasure, the controller in effect assumes responsibility for passing on the request to the other controllers in the supply chain, even if the controller receiving such a request was not the party that obtained the data originally.

Finally, the Advocate General's view was that Article 17(2) of Regulation (EU) 2016/679 did not preclude a national supervisory authority from ordering a provider of directories to inform search engine providers of requests for erasure that it had received. Among other things, the Advocate General suggested that an alternative finding would create a perverse scenario which encourages controllers' dissemination of the data widely in order to limit their responsibilities in processing the personal data.

**Case details:**

- Court: Court of Justice
- Advocate General: Collins
- Date of judgment: 28 April 2022

Marc Dautlich is a partner and Jamie Cox, is an associate, both at Bristows LLP. If you have any questions about membership of our Case Analysis Expert Panels, please contact caseanalysis@lexisnexis.co.uk.