Blockchain: the right to be forgotten (or not)

Dean Armstrong QC & Paul Schwartfeger, 36 Commercial, consider how organisations can & should respond to erasure requests on blockchain

IN BRIEF

▶ The right to erasure under Article 17 under the UK GDPR is not absolute and specialist lawyers ought to be involved in blockchain projects from their outset, to assess their suitability for compliance.

Now that the UK has left the EU and the transition period has ended, the provisions of the EU General Data Protection Regulation (GDPR) no longer strictly apply to the UK, albeit the Regulation's extraterritorial reach continues to affect those offering goods or services to data subjects in the EU. Even for those who only serve individuals in the UK, however, the Regulation's effects continue to be felt, as its provisions have been incorporated into domestic law as the 'UK GDPR'.

Practically speaking, the core data principles, rights and obligations remain largely unchanged as a result of this regulatory switch, and as such this article makes no distinction in its analysis between the EU and UK regimes—either or both of which may apply to a data controller or processor operating within the UK.

Under both, the so-called 'right to be forgotten' (more accurately, the 'right to erasure') is found in Article 17, and, in both, barring some modifications to jurisdiction, the right is essentially the same. As at paragraph 1 of Article 17, a data subject has "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" where one of the grounds listed thereunder applies.

While a data subject's Article 17 right may appear straightforward on its face, the technology-agnostic nature of the GDPR ignores entirely the realities of whether (and how) the right might be realised. Indeed, when it comes to blockchain, this agnosticism creates something of a paradox. That is that, while the right is legally enshrined, it is also seemingly technically impossible to achieve, given the mantra that data stored on a blockchain is immutable. This fundamental issue, having real relevance to public or permissionless blockchains which, for example, underpin Bitcoin and Ethereum, has been the subject of much debate since the inception of the GDPR.

Given this immutability issue, how, then, can data controllers that use blockchain technology comply with their obligations under Article 17? Adopting a more nuanced approach to analysing Article 17 and related issues yields a few possible solutions, as well as some guidance for how data controllers might respond to erasure requests.

The right to erasure is not absolute

As set out in Article 17, the right only applies where one of the specified grounds exists. These include where the personal data is no longer needed; where the lawful basis for processing the data was consent and the data subject withdraws that consent; where the data subject objects and no overriding compelling legitimate grounds for continued processing exist; where the personal data was unlawfully processed in the first place; or where erasure is needed to comply with a legal obligation.

If one of the specified grounds does not exist, then the erasure request may be refused. Some data controllers might, therefore, be able to refuse erasure on the basis that there remain compelling legitimate grounds for the continued processing of the personal data concerned. Given that an individual's control of their personal data is at the heart of the Regulation and its related legislation, this may be a hard hurdle to overcome. (See discussion below.)

Other exceptions to erasure are enumerated in paragraph 3 of Article 17 and include where processing is necessary for the exercise of the right to freedom of expression, for archival purposes that are in the public interest or necessary for statistical purposes, or for the establishment, exercise or defence of legal claims. Certainly, careful consideration of the wording of Article 17 and of the circumstances of the controller's data use is needed to establish whether erasure is necessary at all following an Article 17 request.

What constitutes personal data is open to interpretation

Personal data is defined in Article 4(1) as 'any information relating to an identified or identifiable natural person ("data subject")' where 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

From this it should be clear that anonymised data is not subject to erasure under Article 17 and that a request for such can be refused.

This notwithstanding, the definition of 'personal data', and therefore what must be erased under Article 17, is not entirely clear either and will continue to be something subject to interrogation and resolution through case law.

For example, in *Patrick Breyer v Germany* Case C-582/14, the Court of Justice of the European Union (CJEU) held that IP addresses could constitute personal data in certain circumstances. In *Breyer*, this was where a legal means existed which would enable an online media services provider to identify the data subject who had visited its website from additional data which the data subject's internet service provider held about them. Within a given jurisdiction, the existence and scope of such a 'legal means' may therefore be relevant to whether an IP address (or other data) is 'personal' and therefore comes within the scope of Article 17.

While on the one hand *Breyer* should serve as a warning to controllers of the expansive approach taken by the CJEU to the notion of personal data, it serves also as a reminder that concepts of personal data are open to interpretation. Only where a natural person is or can be identified directly or indirectly from the data concerned is the data likely to be considered personal data and therefore subject to the controls, rights and remedies of the GDPR. Data controllers may

therefore want to analyse the full extent of the data which a data subject seeks to have erased before acting on an erasure request, to establish whether it all comes within the ambit of the GDPR and the erasure requirements of Article 17.

The data might not be immutable after all

Even if obliged to act under Article 17 and the data concerned constitutes personal data, an organisation's use of blockchain technology may not mean it is impossible for them to comply with an erasure request. Blockchains exist in different forms, and different implementations may have a bearing on what is and isn't possible.

One of the typical distinctions made is between a public versus a private blockchain. Public blockchains are open to the public and anyone can participate in the network without needing permission, adding and verifying blocks of data. Consensus protocols between participants ensure that all data stored on the chain is valid. Consequently, an attempt by one participant to erase or overwrite any existing data will be detected by the others and corrected. Immutability is thereby enforced by all network participants and cannot be avoided, which presents obvious compliance challenges when it comes to Article 17.

In a private blockchain, however, only approved participants can take part. Indeed, the blockchain could theoretically be implemented in such a manner that a single organisation has authority over it. As a result, certain architectural principles, including immutability, could feasibly be modified by the system's developers so that data can technically be erased.

Public versus private distinctions aside, a blockchain might also be combined with a conventional database which allows records to be erased or overwritten at will. If the blockchain records only non-personal transactional data, while personal data is stored 'off chain' in a conventional database, the conventional database records could feasibly be erased following an erasure request leaving the blockchain unaltered and intact.

There may also be scope within the requirements of Article 17 to minimise the need for direct action from a data controller following an erasure request, depending on how the blockchain has been implemented.

Under Article 17, data controllers must erase personal data 'without undue delay'. However, ICO guidance on the right to erasure indicates, that, where personal data is stored as a backup and is not used for any other purpose, simply holding the backup until it is replaced in line with an established schedule is unlikely to pose a significant risk (*https://bit.ly/3kghEyK*). One might infer from the ICO's guidance that a system which (say) creates a new blockchain each month to backup transactions to, and which destroys each monthly blockchain backup a month later, is sufficient to avoid any specific erasure action being required on the part of the data controller at the time that an erasure request is received.

Erasure obligations are not necessarily global

Should an organisation be required to erase data pursuant to Article 17, it appears from *Google v CNIL* Case C-507/17 that its erasure obligations might also be territorially constrained.

In *Google*, the CJEU held that it is in no way apparent from the wording of the GDPR that the EU legislature wanted to confer the right to be forgotten beyond the territory of EU member states. Accordingly, while upholding that a search engine operator had to remove links to the pages containing the personal data concerned from its EU search engine results, it was not required by the GDPR to do so from other non-EU versions of its search engine, albeit it would have to prevent or at least seriously discourage an internet user from gaining access to those search results.

Depending on the nature of an organisation's services and the way in which personal data is processed and accessed by it, the Court's ruling in *Google* could potentially limit the territories in which an organisation needs to ensure an erasure request is effective.

Conclusion

The right to erasure under Article 17 is not absolute and the definition of personal data is certainly not settled. A data subject's 'right to be forgotten' under the GDPR will therefore turn on the facts. Even where a valid erasure request is received and needs acting on, the mantra that the blockchain is immutable may not necessarily be true (or relevant) in an individual context, and the specific nature of an organisation's implementation should be considered to establish how the organisation might respond and where any personal data it holds might need to be erased from.

When it comes to blockchain, however, the options for how an organisation responds to an erasure request may very well be determined by the decisions that the organisation made when it implemented its systems. Accordingly, specialist lawyers ought to be involved in blockchain projects from their outset, to assess their suitability for compliance with the GDPR and other relevant regulatory regimes. NLJ

Dean Armstrong QC
https://36group.co.uk/members/dpaqc

Paul Schwartfeger
https://36group.co.uk/members/psc

36 Commercial
Part of The 36 Group, Barristers' Chambers
www.36commercial.co.uk
clerks@36commercial.co.uk