

NOTE FOR MISSING PEOPLE

General Data Protection Regulation (GDPR) "Right to erasure"

Overview of the legal position of formerly missing people who wish to have information about them removed from the internet and/or excluded from internet searches

This note was created for the purpose of providing legal advice to Missing People Ltd only. Missing People Ltd may disclose this note to, or discuss this note with, formerly missing people (who wish to exercise their right to erasure and have information about them removed from the internet and/or excluded from internet searches) and their representatives, as well as organisations (e.g. search engine operators) with which such requests for erasure are discussed. However, no recipient of this note other than Missing People Ltd may rely on this note as legal advice.

1. PURPOSE OF THIS NOTE

This note gives an overview of the legal position and the rights of individuals who:

- (a) have been reported as missing in the past but are no longer missing;
- (b) have had personal information about them released on the internet during the time they were missing (e.g. through a missing person appeal, articles in local media websites or posts on social media platforms); and
- (c) want that information deleted from the internet or excluded from internet search results.

2. WHAT IS THE RIGHT TO ERASURE?

- 2.1 The General Data Protection Regulation (GDPR) sets out how organisations need to handle personal data. In this context, "personal data" means any information that can identify the individual (directly or indirectly) - e.g. a name, a photograph that clearly shows the face of the individual, or a location where the individual was last seen.
- 2.2 Article 17 of the GDPR gives individuals (both adults and children) the right to have their personal data erased in some circumstances. This right is known as the 'right to erasure' (also known as 'the right to be forgotten'), and applies in circumstances where, although the original collection and processing of the data may have been compliant with the GDPR, continuing to hold or publish the personal data is not. In these circumstances, individuals can prevent organisations from continuing to make their personal data available on the internet or in other contexts (e.g., to keep a missing

person appeal on a website or social media platform, or to show a link to such a page in the results of a search carried out using an internet search engine such as Google).

- 2.3 The right is exercisable by contacting the organisation that publishes the data, or runs the search engine, and requiring it to erase the data.
- 2.4 The circumstances allowing exercise of the right to erasure that are most likely to apply in the context are where:

- (a) **the personal data are no longer necessary given the purpose for which they were collected or processed** (Article 17(1)(a)).

This relates closely to one of the GDPR's basic principles governing all processing personal data (given in Article 5(1)(e)). Personal data should not be kept in a form which allows identification of the individual for longer than is necessary given the purposes for which the data are processed.

For example, it could be argued that a missing person appeal, originally posted on the internet to help find the individual, is no longer necessary (and therefore, should be erased) once the missing person is found.

In this circumstance, the organisation should not wait for a request from the individual but should cease processing the data of its own accord. The right to erasure is effectively a mechanism for reminding the organisation of its existing obligation to cease processing the data.

- (b) **the individual has exercised his or her right to object to the continued processing of his or her personal data and the organisation** (e.g. a local media website, social media platform or search engine provider) **has no "compelling legitimate grounds" for continuing the processing** (Article 17(1)(c), with the right to object arising separately, under Article 21(1)).

In this circumstance, the organisation's reasons for keeping the data on the internet and the public's interest in having access to the data (if any) must be balanced against the interests, rights and freedoms of the individual. The organisation has to demonstrate compelling reasons for continuing to process (in this case, to publish) the data. If it cannot, it should delete the data.

- 2.5 In practice, individuals exercising the right to erasure rely on **both** Article 17(1)(a) **and** Article 17(1)(c). Article 17(1)(a) only applies where the organisation really has no reason for continuing to publish the data. Article 17(1)(c) allows the individual to argue that the organisations reasons for continuing to publish the data are not sufficiently "compelling" to override the harm that it is causing to their interests, rights and freedoms. The more significant the damage or distress caused to the individual by the continued processing of their data, the more likely it is that the organisation will be obliged to erase the data.

- 2.6 In order to rely on Article 17(1)(c), the individual should first "object" to the continued processing of their data, exercising the right under Article 21(1), and then require the data to be erased. In practice, the two rights can be exercised together, in a single communication to the responsible organisation.
- 2.7 The right of erasure does not arise if the continued processing of the data is "necessary for exercising the right of freedom of expression and information" (Article 17(3)). The UK Data Protection Act 2018 (at paragraph 26 of Schedule 2) expands on this exception, specifying that the right of does not apply to personal data processed for journalistic purposes with a view to publication, where the organisation reasonably believes that publication (in this case, *continued* publication) is in the public interest. This exception will need to be taken into account wherever requests are made to erase personal data published in a journalistic context, for example on a newspaper's internet page. Requests to take down articles from news media are likely to be resisted, although items focussed entirely on furthering an appeal to find a missing person, rather than reporting on the circumstances of their disappearance in a journalistic manner, might still be taken down. Note, further, that this exception will not generally allow the operator of a search engine to refuse to exclude links to journalistic materials from its search results – although it may still refuse to exclude links if it considers that there is a strong public interest in continued publication.
- 2.8 Other circumstances that give rise to the right to erasure (but are less likely to apply in the context) are:
- (a) **where the individual withdraws his or her consent for the personal data to be processed** (Article 17(1)(b)). It is unlikely that a formerly missing person will have consented to the publication of their personal data (e.g. in a form of a missing person appeal) – the organisation will be processing their personal data on a legal basis other than consent, so this circumstance is unlikely to arise.
 - (b) **Where the personal data have been processed in breach of the GDPR** (Article 17(1)(d)). This may apply, but the missing person will not generally know whether it is the case or not.
 - (c) **Where the personal data must be erased for compliance with a legal obligation** (Article 17(1)(e)). Few if any legal obligations to erase, other than those arising under the GDPR itself, are likely to be relevant in practice.
 - (d) **Where the personal data have been processed in the context of offering information society services (ISS) to a child** (Article 17(1)(f)). This is intended to allow under-age users of social media and similar services to require personal data that they have posted to be taken down.

3. THE ORGANISATION'S RESPONSIBILITIES

- 3.1 If one of the circumstances discussed in paragraph 2 applies and the formerly missing person exercises the right to erasure, the organisation must erase the personal data (Article 17(2)).

- 3.2 Where the organisation has made the personal data public on the internet, it should take reasonable steps to inform others who are processing the personal data to erase links to, copies or replication of that data. "Reasonable steps" will be determined taking into account the available technology and the cost of implementation (Article 17(2)).
- 3.3 If the organisation believes that it does not need to erase the information, it should explain why and inform the individual that they can make a complaint to the Information Commissioner's Office (ICO). The ICO is the UK's independent body that upholds data privacy rights for individuals and has a range of powers which it can exercise against organisations refusing to respect the right to erasure, including a power to impose very substantial fines.

4. **WHEN THE RIGHT TO ERASURE DOES NOT APPLY**

- 4.1 In addition to the journalistic exception discussed in paragraph 2.7 above, the right to erasure also does not apply where continued publication of the personal data is necessary for:
- (a) compliance with a legal obligation;
 - (b) performance of public interest or exercise of official authority;
 - (c) public health reasons;
 - (d) archiving, research or statistical purposes; or
 - (e) establishing, exercising or defending legal claims.

These exceptions are, however, unlikely to be relevant to the circumstances discussed in this note.

- 4.2 **Note on jurisdiction / geography:** some non-UK/non-EU organisations may argue that they are not subject to the GDPR at all and are therefore not obliged to respond to requests for erasure. These arguments need to be considered on a case-by-case basis. Courts and regulators are inclined to take an expansive view of the geographical application of UK and EU data protection law and, for example, have held that Google (based in the US) is subject to the right to be forgotten because its search engine supports its advertising business in the EU.

5. **CHILDREN**

- 5.1 The GDPR gives enhanced protection of children's information (especially in online environments), and there is an emphasis on the right to have children's personal data erased. Therefore, an organisation is more likely to give weight (and less likely to object) to a request for erasure if the information relates to a child. This will still be the case where a formerly missing person is now an adult, but was a child at the time when they were missing. None of this means that an organisation should not honour a request for erasure from an individual who was an adult when missing.

5.2 The GDPR does not specify the age at which children are competent to exercise their rights under the GDPR in their own right. ICO guidance provides that a child may exercise the rights (including the right to erasure) "on their own behalf as long as they are competent to do so". It also provides that, "in Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases".

5.3 If a child is too young to exercise their rights themselves, a parent (or holder of parental responsibility) can make the request for erasure on their behalf (provided this is in the child's best interest). If in doubt, it makes sense for the child and a parent or holder of parental responsibility to make the request jointly.

6. WHAT INDIVIDUALS CAN DO TO REQUEST ERASURE

6.1 There are different ways in which the individual can attempt to have his or her personal data erased from the internet:

(a) **Erasure at source:** *an example:* an individual sees that their missing person appeal is still published on a local media webpage. The individual can contact the local media webpage to request erasure. If the request is successful, the missing person appeal is erased from the website.

(b) **Delisting:** *an example:* when an individual's name is searched on a search engine, the search results include links to a missing person appeal on a local media webpage. The individual can contact the search engine and request that the search result is removed from future similar searches. This may reduce the likelihood of others finding the particular missing person appeal, and a single request can be made to a search engine operator for removal of multiple links from search results. Even if the erasure request is successful, however, this does not mean that the data will be deleted at source (i.e., in this example, the missing person appeal will remain on the local media webpage, but subsequent searches against the formerly missing person's name on that search engine will not find it).

6.2 An individual can make an erasure request to an organisation either orally or in writing (including by email), and the request does not have to be addressed to any particular person within an organisation or to use any particular form of words. In practice, however, it is better to make requests in writing, referring expressly to the GDPR's objection and erasure rights, to be as specific as possible as to the materials (or search results) to be erased, and to address the request to a person within the organisation who is responsible for dealing with the exercise of GDPR data subject rights or with data protection issues generally, so as to maximise the likelihood of a swift and satisfactory response.

6.3 An individual can authorise someone else to make a request on their behalf (including a representative such as a charity or a solicitor).

- 6.4 An organisation must respond to a request for erasure "without undue delay" and in any case within 1 month of receiving the request. The organisation can extend this response time by additional 2 months if the request is complex or, in some circumstances, if the individual sends multiple requests, but in such a case, it must: (i) notify the individual without undue delay and in any case within 1 month of receiving the request, and (ii) explain why they need the extension.
- 6.5 Some organisations have a standard process in place to handle erasure requests. For example, Google has a "Personal Information Removal Request Form" (https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&hl=en&rd=1). The form allows an individual to request specific results from a Google search (for queries that include his or her name) to be deleted.

7. **BREXIT**

Brexit will not affect the right to erasure – the European Union (Withdrawal) Act 2018 will effectively convert the GDPR into UK legislation immediately when Brexit takes effect, and individuals in the UK will still have the right to exercise the right to erasure under the GDPR against EU organisations.

05 November 2018