|  |  |  |
| --- | --- | --- |
|  | | |
| **Document: DSR-03-**Release V1.4 | **UK GDPR - Data Subject Rights – The Right to Erasure** | 08.02.2024 |
| **Authorised by:** Jackie Neil | |  |

**Introduction**

The UK GDPR provides for the rights of a natural person over the information that is held on them. The Right to Erasure, sometimes known as the Right to be Forgotten, enables the data subject to enforce data controllers and data processors to remove personal information about them. The reasons for requests for erasure range from removal from mailing lists that may be a nuisance to the data subject to removal of information that may prejudice the rights of the data subject.

**Overview**

When a data subject notifies the Data Controller either directly or indirectly via staff, data processors, sub processors etc., that they require information to be permanently removed, a record of the notification should be made and time-stamped. The ICO is clear that there is no requirement for a formal template for a right to erasure request. The Data Controller is responsible for satisfying the request, so it is important that all parties involved in the data management lifecycle are made aware of this procedure. If you have a Data Protection Officer (DPO), they must be informed when data subject requests are made so that they can monitor progress.

**Prerequisites**

In order to fulfil an erasure request, the Data Controller must understand what data is specifically under question. In some circumstances, the data subject may require a sub-set of information to be erased. For example, there have been requests made of search engine companies to erase details of spent convictions from search results. Understanding the full extent of the request may save time, effort and misunderstanding. The responsibility for erasure must fall to a nominated person or their delegate even if they are not personally responsible for the actual data removal from a technical perspective. As there are time limitations, knowledge of data management is essential in order to streamline the process. A data mapping process across the organisation should be performed to help identify where information resides both on-site and with any contracted third parties such as Information Systems providers, this will ensure that any ‘upstream’ or ‘downstream’ data repositories can be addressed, this includes data backup services.

**Scope & Limitations**

Although the right of the data subject for personal information to be removed by the Data Controller is enacted within the Data Protection Act 2018, there are considerations that must be made prior to removal of the information:

* Validation of the requestor’s identity where the request is made in person
* Validation of the data subject’s authority where the request is made by a representative such as a lawyer
* A review of information to ensure that the data requested for deletion is not subject to data retention requirements pertaining to superseding law or regulations, for example the current fostering regulations or tax law
* Where the Data Controller has the right to retain the data subject’s personal information to maintain a contractual agreement such as a financial arrangement
* Where the deletion may impact the rights and freedoms of other data subjects, for example where two or more data subjects’ personal information is contained within the same data record. In this situation pseudonymisation or redaction may be necessary to comply with the request.

**Erasure of Information**

Information must be erased only upon consideration of the scope and limitations listed above. Once it is clear that information is in scope and that the requestor is within their rights to erasure, the information must be deleted without delay. The data must be removed from all services and systems, including paper records to ensure completion.

It is appropriate to advise the requestor once the deletion process is complete.

**Time Frame**

Requests for erasure must be acknowledged promptly, this can be accomplished during the identity verification stage. The overall process should be completed within 28 days from the day after the request is received. If you are unable to remove information directly, for example on a back-up copy of the information that is subject to an overwrite process and where individual records cannot be edited without affecting the integrity of other information, notify the data subject of the technical limitations and record the exception inthe central register. A commitment to pseudonymise or to ‘cease processing’ should be made to the data subject where it is technically infeasible to delete information.

**Procedure**

1. Data subjects must make their request to the Data Controller (this can be any representative of the Data Controller). Where a data subject makes a request to any member of staff, volunteer, contingent worker or third party processor, the request must be directed to the nominated staff member responsible for requests and this direction must be confirmed via a letter or an email to both the data subject and the responsible person. If you have a DPO, they must also be informed of the request and kept informed of the request status throughout the process.
2. The details of the request will be entered in a Data Subject Rights register. This will enable tracking to ensure timelines are adhered to.
3. Upon receipt of the request, the data controller must make all reasonable efforts to validate the identity of the requestor to ensure they have a legal right to erasure of the information requested.
4. Once the data subject’s identity is validated, the controller will consult with the data subject to verify the data deletion requirement.
5. The controller will use the services of data processing staff or services to remove any additional or external copies of the information whether electronic or paper based. Unless it falls outside the terms stated in the section headed ‘Scope & Limitations’.
6. Within 28 days of the request, the controller will ensure that all copies of the information under dispute is deleted where technically feasible. Systems where information cannot be deleted will be amended to either de-identify the information using pseudonymisation or processing of the data will be ceased. A record of the actions committed will be listed in the central register.
7. Where information cannot be deleted within 28 days of the request, the data subject will be notified that additional time is required along with the reason for delay and anticipated time for completion. Where information cannot be deleted due to technical limitations, the data subject will be informed of the lack of completion and that the limitation of the request has been recorded in the central register.
8. The Data Subject Rights register will be updated to conclude the request activity.

A complete data map will be required to provide the data controller with the necessary information to conduct this procedure effectively. Data retained by any third-party processors must be included in this process with attestations from them when deletion is complete.