|  |
| --- |
|  |
| **Document: DSR-06-**Release V1.4 | **UK GDPR - Data Subject Rights – The Right to Object** | 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 Object allows for data subjects to have an absolute right to stop their data being used for marketing, which is the most common use of the right. Data subjects also have the right to object to other types of data processing but where marketing is not the purpose, the request can be challenged where the controller/processor can demonstrate an overriding purpose.

**Overview**

When a data subject notifies the Data Controller either directly or indirectly via staff, data processors, sub processors etc., that they object to the processing of their information, 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 restriction of processing 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 restriction requests are made so that they can monitor progress.

**Prerequisites**

In order to fulfil a right to object 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 restricted for processing. For example, there may be information that is required to be maintained to support a contractual requirement, but that information is also used to provide marketing information to the data subject. The data subject has the right to object to the data being used for marketing, but not for the execution of a contract. 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.

**Scope & Limitations**

Although the right of the data subject to object to their personal information to be processed 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
* You may not refuse the request if the purpose for processing information is direct marketing, even if prior consent has been given
* You may refuse the request if you have compelling legitimate grounds for processing the data or the processing is for the establishment, exercise or defence of legal claims.

**Objection to Information Processing**

The right to object to Information processing must be satisfied 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 object to processing, the request must be attended to without delay. The data processing must be stopped for all in-scope services and systems.

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

**Time Frame**

Requests 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 cease processing information directly, notify the data subject of the technical limitations and record the exception in the central register.

**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 object to information processing as requested.
4. Once the data subject’s identity is validated, the controller will consult with the data subject to verify the scope of the requirement.
5. The controller will use the services of data processing staff or services to cease processing the information, unless it falls outside the terms stated in the section headed ‘Scope & Limitations’. It is important to ensure that any third-party processors also comply with the request for data within scope.
6. Within 28 days of the request, the controller will ensure that processing of the information subject to the request is ceased. This can be done, for example by moving the information to another system that is inaccessible to the processing function. A record of the actions committed will be listed in the central register.
7. Where information processing cannot be ceased 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 processing cannot be ceased 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 compliant actions are complete.