|  |  |  |
| --- | --- | --- |
|  | | |
| **Document: DSR-01-**Release V1.4 | **UK GDPR - Data Subject Rights – The Right of Access** | 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 of Access is one of the most commonly exercised rights; it enables data subjects to gain access to information held about them by organisations acting as Data Controllers, Joint Data Controllers, Data Processors and Data Sub-Processors.

**Overview**

When a data subject requires access to information held on them, the request is called a Data Subject Access Request or, more commonly, a Subject Access Request (SAR). The ICO is clear that there is no requirement for a formal template for a SAR so where a data subject requests information from any staff member, it should be considered a SAR. The Data Controller is responsible for satisfying the SAR, so it is important that all parties involved in the data management lifecycle are made aware of this procedure. No charge can be made to the data subject in the provision of this service unless multiple requests are made or where it is clear that the attempt to gain information is being made to create a ‘nuisance’ to the Data Controller. As requests are tracked and monitored, multiple requests from individuals will become apparent.

**Prerequisites**

In order to fulfil a SAR, the Data Controller must understand where data is held, for that reason, the responsibility of completion must fall to a nominated person or their delegate. 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.

**Scope & Limitations**

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

* The Local Authority must be consulted for requests concerning looked after children as there may be ongoing LADO investigations and the LA may be the data controller for some elements of children’s data
* Validation of the requestor’s identity must be made where the request is made in person. Extra vigilance is recommended when the request is made by a child e.g., a carer’s birth child to ensure the authenticity of the request.
* 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 no ‘legally privileged’ information is disclosed
* Information that, if disclosed, would prejudice the rights and freedoms of another data subject within specific documents is exempted from the information to be made available to the data subject, for example, confidential references.

If your organisation has identified a Data Protection Officer (DPO), they must be advised that a SAR has been requested.

**Provision of Information**

Information must be delivered to the data subject in a ‘durable format’ This means that the data should be provided in a common machine-readable file(s) made available via a secure internet connection, on a secure USB thumb drive or printed on paper. Understanding the needs of the data subject is important so identifying their preferred medium is advised. The data must be available to the data subject for a ‘reasonable’ period of time. It is advised to have the information available for a period of 90 days before deletion and the data subject must be made aware of this time restriction.

Information that is for general consumption, where the data subject has been included in a distribution list, is not in scope. For example, where the data subject is an employee and they are included in an email to all staff describing a new fire drill procedure, the information is not ‘about’ the data subject and so is out of scope.

**Time Frame**

SAR’s 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 SAR is received. If you are unable to provide all the information within this timeframe, you must provide all of the information that is available and signal to the data subject that you will complete the provision of information in good time. The limit considered acceptable to manage the remainder of the information is 90 days according to the ICO.

**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 SARs 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 acquire copies of the information requested.
4. Once the data subject’s identity is validated, the controller will consult with the data subject to define the scope of the data subject’s requirement and acknowledge the request scope within a time limit of 24 hours.
5. The controller will use the services of internal data processing staff or external processor services to acquire the information pertaining to the data subject. Consideration to be afforded to the terms stated in the section headed ‘Scope & Limitations’. In particular, where other Data Subject’s information may be disclosed redaction of that information may be applied.
6. Within 28 days of the request, the controller will provide a copy of the information permitted for disclosure to the data subject in an open-source format (PDF etc) on a standard USB drive, to be posted using recorded delivery by the Royal Mail.
7. Where information cannot be provided within 28 days of the request, the data subject will be notified that additional information may be provided to them at a date not exceeding 90 days from the original request.
8. A copy of the contents of the USB drive will be retained for a period of three months to ensure the data subject has sufficient time to acquire additional copies or to challenge the content of the disclosure. A calendar entry will be created 90 days after the disclosure to advise the data controller to delete the information.
9. After a period of three months has elapsed, the retained copy of the disclosed information held will be deleted and the data subject will be notified of the data deletion in writing, posted using recorded delivery by the Royal Mail.
10. The Data Subject Rights register will be updated to conclude the request activity.

SARs are often requested in response to a dispute or to challenge a decision. It is imperative that information is provided ‘without prejudice’ and is complete notwithstanding the provisions made in the section headed ‘Scope & Limitations’.