Independent Commission for Reconciliation and Information Recovery

Subject Rights Request Policy

September 2024

Version	Issue Date	Last review date	Owned by
1	September 2024	September 2024	ICRIR Data

1. Introduction

1.1 Under the UK General Data Protection Regulation ("**UK GDPR**"), individuals have rights in relation to their Personal Data. "Personal Data" is defined as any information relating to an identified or identifiable natural person. Individuals are able to exercise their rights by making Subject Rights Requests ("**SRRs**") to the organisations or "Controllers" which hold their Personal Data.

1.2 In order to provide information to victims and survivors and families of Troubles-related deaths and serious injury and to promote reconciliation, the Independent Commission for Reconciliation and Information Recovery ("**ICRIR**", **we**", "**us**" and "**our**") is required to collect and process Personal Data. Both our internal and external-facing Privacy Notices contain detailed information about the categories of individuals we will collect Personal Data from ("**Data Subjects**"), and the purposes for which we may process it. What is relevant for the purposes of this Subject Rights Request Policy ("**Policy"**) is that from time to time we may receive SRRs, and it is important we have a lawful and consistent process in place for responding to these.

1.3 The purpose of this Policy is to identify the rights that Data Subjects have in relation to their Personal Data, and to outline how we will respond to SRRs in accordance with our legal obligations. This includes, but is not limited to, the UK GDPR and the Data Protection Act 2018 ("**DPA 2018**"). It is important that you are aware that failure to comply with this Policy could expose us to fines, penalties and reputational damage, not to mention the impact it may have on Data Subjects. As such, failure to comply with this Policy will be dealt with in line with the ICRIR Conduct and Discipline Policy.

2. Recognising and recording SRRs

2.1 SRRs can be made to any individual or part of our organisation. We are all responsible for recognising SRRs, ensuring they are dealt with in line with this Policy and complying with applicable law.

2.2 SRRs can be in any form, including verbally, in writing, via email or through social media. Of note, SRRs do not have to specifically refer to "Personal Data" or the "UK GDPR" in order to be valid. What is important is whether a request by a Data Subject relates to their rights in relation to their Personal Data. This means that requests for "information" we hold about Data Subjects will be in scope, as will others of a similar nature. For this reason, it is important you familiarise yourself with the rights outlined in this Policy so that you are able to identify any such requests.

2.3 So that we are able to both monitor and demonstrate our compliance with the UK GDPR, it is important that we keep accurate records of all SRRs that we receive and how we respond to them. This should be done through our SRR Register. At a minimum, the following information ought to be recorded:

2.3.1 the date on which the SRR was received;

2.3.2 the identity of the Data Subject;

2.3.3 the nature of the SRR, and any concerns you identified in complying with it;

2.3.4 the date on which you responded to the SRR; and

2.3.5 a description of:

2.3.5.1 what Personal Data or information you provided in response to the SRR, if any; and

2.3.5.2 whether you relied upon any exemptions as providing the organisation with a lawful basis for declining to provide Personal Data or information in response to the SRR.

2.4 If you have any questions about what information ought to be recorded, please contact our Data Protection Officer ("**DPO**") for assistance, whose details are set out at the end of this Policy. Our DPO is the person within our organisation with overall responsibility for providing us with information and advice about the processing we undertake, monitoring our compliance with the UK GDPR and other laws relating to the protection of Personal Data, and acting as a point of contact for the ICO in relation to any issues that may arise.

3. General requirements

3.1 You must immediately (i.e. within one working day) notify our DPO of any SRR you receive, or any request you suspect may qualify as a SRR. This is important for the reasons following:

3.1.1 firstly, to ensure we have sufficient time to decide who should respond to the SRR;

3.1.2 secondly, to ensure we comply with the timeframes imposed by the UK GDPR for responding to SRRs; and

3.1.3 lastly, to ensure we deal with SRRs consistently, in compliance with this Policy and applicable law, so as to reduce the risk of Data Subjects receiving different responses and information from different staff members.

3.2 Before responding to or acting on a SRR, we must be satisfied that the individual who has made the SRR is the Data Subject who they claim to be. In some cases, we may need to request written evidence or verification. What is reasonable will vary on a case by case basis. This is a security measure to ensure that we do not, for example, provide an individual with access to the Personal Data of a Data Subject which they have no right to receive.

3.3 In addition to the above, in some limited circumstances third parties are

able to make SRRs on behalf of Data Subjects. This could include the legal representative of a Data Subject, or a friend or family member. Where an individual purports to be making an SRR on a Data Subject's behalf, we must again be satisfied that they have the lawful authority to do so, and make reasonable enquiries in this regard. Our DPO will be able to provide you support as to what is needed on a case by case basis.

3.4 Once satisfied of the identity of the Data Subject or of the lawful authority of a third party to act on their behalf, we must make all reasonable efforts to comply with their SRR. Depending on the nature of the SRR this may involve searching our databases, systems, applications and other places where we store Personal Data. The timeframe imposed by the UK GDPR for responding to a SRRs is one calendar month. If however an SRR is practically complex and we need to extend this timeframe, we are required to inform the Data Subject of our reasons for this, and ensure we are doing all that we can to comply with their SRR as soon as is reasonably practicable.

3.5 When responding to SRRs, we must communicate in a concise, transparent, intelligible and easily accessible form, and use clear and plain language. We should generally communicate in writing (which can include email) but we can reply verbally if specifically requested by the Data Subject to do so. If we are going to decline to comply with the SRR, we should inform the Data Subject of our reasons for this, unless an exemption to that obligation applies (see paragraphs 4.4 and 4.5 for further detail on this), and of the possibility of their right to make a complaint to the Information Commissioner's Office ("**ICO**").

3.6 Please note that if an SRR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee which takes account of the administrative costs of providing or transmitting Personal Data. You should also seek written approval from our DPO before charging any such fee, and to confirm the

amount you have proposed is appropriate in the circumstances.

3.7 Lastly, you should always seek guidance from our DPO, and obtain their written approval before responding to a SRR, but especially so in circumstances where an exemption may apply.

4. Right of access

4.1 Subject to some limited exemptions (discussed at paragraphs 4.3 and 11), individuals have the right to seek confirmation as to whether we hold their Personal Data, and where this is the case, they have the right to receive it. This type of SRR is commonly referred to as a Subject Access Request, or a "**SAR**". Generally, there is no fee associated with this. However, we may charge a reasonable fee or refuse to comply with a SAR if it is clearly unfounded, repetitive or excessive.

4.2 As well as being entitled to access their Personal Data, Data Subjects are also entitled to the following information:

4.2.1 the type of Personal Data we hold for them;

4.2.2 the purposes for which we use their Personal Data;

4.2.3 if the Personal Data we hold about you was not provided by the Data Subject, details of the source of the information;

4.2.4 who their Personal Data has been or will be shared with, including in particular organisations based outside the UK;

4.2.5 if their Personal Data leaves the UK, how we make sure that it is protected;

4.2.6 where possible, the length of time we expect to hold their Personal Data;

4.2.7 whether we make any automated decisions in respect of their Personal Data;

4.2.8 regarding their right to ask us to amend or delete their Personal Data;

4.2.9 regarding their right to ask us to restrict how their Personal Data

is used or to object to our use of their Personal Data; and

4.2.10 regarding their right to complain to the ICO.

4.3 As mentioned at paragraph 4.1, there are some limited exemptions to the right of access. In the context of SARs, the most common one to arise is that the Personal Data the Data Subject has requested includes the Personal Data of another individual. Before responding to a SAR therefore, we must carefully review the Personal Data within the scope of the SAR to determine whether it includes the Personal Data of any other individual. If so, we will need to consider:

4.3.1 whether it is possible to redact this Personal Data;

4.3.2 whether the other individual would be comfortable consenting to the disclosure of their Personal Data; or

4.3.3 whether it would nonetheless be reasonable to disclose without the other individual's consent.

4.4 In addition, and particularly in light of the type of information collected by the ICRIR and its functions, certain Personal Data may also be exempt from the right of access in circumstances where national security may be compromised. In essence, the right of access can effectively be disapplied in circumstances where it is reasonably necessary to do so in order to safeguard or otherwise protect national security. Examples may include:

4.4.1 protection against specific threats, such as from terrorists or hostile states;

4.4.2 protection of potential targets even in the absence of specific threats; and

4.4.3 international co-operation with other countries.

4.5 Typically, the Data Subject should be informed that some or all (as applicable) of the Personal Data they have requested cannot be provided on the basis of national security. That is, however, unless informing them of that fact would itself undermine the safeguard or protection of national

security.

5. Requests for rectification

5.1 We are required to take reasonable steps to ensure the Personal Data we hold about Data Subjects is accurate and complete. Data Subjects also have the right to request that any inaccurate Personal Data we hold about them is rectified, or completed if incomplete.

5.2 Upon receiving a SRR for rectification, we must consider whether it is reasonable. We cannot, for example, amend the Personal Data we hold simply because the Data Subject disagrees with it, or would like it to be recorded differently. If a Data Subject asks for their Personal Data to be rectified, but we do not agree with their assessment, we should record their request alongside their Personal Data.

5.3 In circumstances where we do rectify the Personal Data we hold, whether in response to a SRR or otherwise, we are required to notify any third party recipient to whom we previously disclosed the Personal Data to, unless it would not be practicable to do so.

5.4 The exemptions relating to national security, as discussed in paragraphs 4.4 and 4.5 above, similarly apply to requests for rectification.

6. Requests for erasure

6.1 Data Subjects have the right to request that we erase the Personal Data we hold about them. This is also known as the 'right to be forgotten'. Unless an exemption applies (discussed further below), we should comply with the request without undue delay provided that at least one of the following conditions is met:

6.1.1 the Personal Data is no longer necessary for the purposes we collected or processed it for;

6.1.2 consent was the lawful basis we relied upon for holding or further processing the Personal Data, and there is no other lawful basis for continue to hold or further process it;

6.1.3 the Data Subject objects to us processing their Personal Data: (i) in our performance of a task carried out in the public interest; (ii) in the exercise of official authority vested in us; or (iii) on the basis of our legitimate interests;

6.1.4 the Personal Data has been unlawfully processed;

6.1.5 we are required to erase the Personal Data so as to comply with a legal obligation to which we are subject; or

6.1.6 the Personal Data was been collected in relation to the offer of information society services.

6.2 There are some exemptions to the right to erasure that provide us with a lawful basis for declining to comply. These are that it is necessary for us to continue to hold or further process the Data Subject's Personal Data:

6.2.1 to exercise the right of freedom of expression and information;

6.2.2 to comply with a legal obligation which requires us to do so, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;

6.2.3 for reasons of public interest in the area of public health;

6.2.4 for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

6.2.5 for the establishment, exercise or defence of legal claims.

6.3 The exemptions relating to national security, as discussed in paragraphs 4.4 and 4.5 above, similarly apply to requests for erasure.

7. Restricting processing

7.1 Data Subjects have the right to request that we restrict our processing of their Personal Data. This could include, for example, a request that we

cease processing their Personal Data for a certain period of time. Provided at least one of the following conditions is met, we must stop processing the Data Subject's Personal Data (with the exception of holding it) without undue delay:

7.1.1 the Data Subject contests the accuracy of their Personal Data, for a period to allow us to verify the accuracy of the Personal Data;

7.1.2 the processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;

7.1.3 we no longer need the personal data for the purposes we collected it, but it is required by the Data Subject for the establishment, exercise or defence of legal claims; or

7.1.4 the Data Subject has objected to the processing, pending verification of whether we have legitimate grounds to override the Data Subject's objection.

7.2 Where a Data Subject has requested that we restrict our processing of their Personal Data, and we have complied with this request, we are only permitted to further process their Personal Data: (i) with the Data Subject's consent; (ii) for the establishment, exercise or defence of a legal claim; (iii) for the protection of the rights of another individual; or (iv) for reasons of important public interest. If we intend to further process the Data Subject's Personal Data in reliance on one of these grounds, we are required to inform them before doing so, unless it would not be it would not be practicable to do so.

7.3 The exemptions relating to national security, as discussed in paragraphs 4.4 and 4.5 above, similarly apply to requests to restrict processing of Personal Data.

8. Portability of Personal Data

8.1 Data Subjects have the right to receive copies of any Personal Data which they personally provided to us in a structured, commonly used and machine-readable format, so that they can transmit it to another Data Controller. We are required to comply with these requests where:

8.1.1 our legal basis for the processing their Personal Data is consent or performance of a contract; and

8.1.2 our processing of their Personal Data is automated.

8.2 Of note, where technically feasible we are also required to transmit Data Subjects' Personal Data directly to other Data Controllers at their request.

9. Right to object

9.1 Data Subjects have the right to object to us processing their Personal Data where the legal basis we rely on for doing so that processing is necessary: (i) for the performance of a task carried out either in the public interest or in the exercise of official authority vested in us; or (ii) for the purposes of our own legitimate interests. The UK GDPR does however provide exemptions to this which permit us to continue to process Personal Data if either:

9.1.1 we can show compelling legitimate grounds for the processing which override the Data Subject's own interests, rights and freedoms; or

9.1.2 we are processing the Personal Data for the establishment, exercise or defence of legal claims.

9.2 In addition to the above, Data Subjects also have an absolute right to object to their Personal Data being processed for marketing purposes (which may include their inclusion in any mailing list). Where Data Subjects' exercise this right, we cannot argue it is outweighed by any competing interest we may have in processing their Personal Data.

10. Automated decision-making

10.1 Data Subjects have the right to not be subject to solely automated decisions. An automated decision is one that is made by a computer without any human input, using their Personal Data, that has a legal or other significant effect on them. We do not carry out automated decision-making.

11. Exemptions

11.1 In most cases, Data Subjects' rights are not absolute. The UK GDPR and DPA 2018 provide several exemptions to these rights which give Data Controllers a lawful basis for declining to comply with SRRs, where applicable. These exemptions are detailed in Schedules 2 – 4 of the DPA 2018, and are in addition to those which are built in to the UK GDPR and apply to specific rights, which we have already summarised above. The exemptions fall into the following categories:

11.1.1 crime, law and public protection;

11.1.2 regulation, parliament and the judiciary;

11.1.3 journalism, research and archiving;

11.1.4 health, social work, education and child abuse;

11.1.5 finance, management and negotiations; and

11.1.6 reference and exams.

11.2 Of the above, it is worthwhile noting that some of the information we collect or receive may be relevant to the prosecution of offences. As such, the 'crime' exemption set out under Schedule 2, paragraph 2 of the DPA 2018 ought to be front of mind when we respond to SRRs.

11.3 A Data Controller's ability to rely on an exemption will generally depend on the purpose for which they are processing Personal Data, and whether it would be desirable and proportionate to comply with an SRR or not, having regard to all relevant circumstances. Before responding to SRR that you have been asked to handle therefore, it is important you

consider whether any exemption may apply, seeking input from our DPO as needed.

11.4 Lastly, please note that these exemptions should not be routinely relied upon, nor applied in a blanket fashion. SRRs should always be considered on a case-by-case basis, with regard to the nature of the SRR, the individual circumstances of the Data Subject and the implications of complying or declining to comply.

12. Further information

12.1 As noted at paragraph 2.4, our DPO is the person responsible for overseeing this Policy, and our compliance with laws relating to the processing Personal Data. Please do not hesitate to contact them if you would like further information about the matters addressed in this Policy. Our DPO is contactable at data@icrir.independent-inquiry.uk.

12.2 Lastly, please note that our DPO will review this Policy on an annual basis, or sooner should the need arise, to ensure it remains fit for purpose. This Policy was last reviewed in September 2024.