Data Subject Request Procedure

Version:	**1.0**
Dated:	**02 May 2018**
Document Owner:	**Information Governance Manager**

Revision History

Version	Date	Revision Author	Summary of Changes
1.0	April 2018	D Bristow / R Platt	Procedures to include all GDPR information rights

Approval

Name	Date
Information Governance and Security Steering Group	May 2018

Contents

List of Figures

List of Tables

1 Introduction

This procedure is intended to be used when a data subject exercises one or more of the rights they are granted under the European Union General Data Protection Regulation (GDPR).

Each of the rights involved has its own specific aspects and challenges to the University of Exeter in complying with them and doing so within the required timescales. In general, a proactive approach will be taken that places as much control over personal data in the hands of the data subject as possible, with a minimum amount of intervention or involvement required on the part of the University of Exeter.

However, in some cases there is a decision-making process to be followed by the University of Exeter regarding whether a request will be allowed or not; where this is the case, the steps involved in these decisions are explained in this document.

This procedure should be considered in conjunction with the following related documents:

- *Data Subject Request Register*
- *Data Protection Impact Assessment Procedure*
- *Records Retention and Protection Policy*
- *Privacy and Personal Data Protection Policy*
- *Legitimate Interest Assessment Procedure*
- *Privacy Notice Procedure*

2 Data Subject Request Procedure

2.1 General Points

The following general points apply to all of the requests described in this document and are based on *Article 12* of the GDPR:

1. Information shall be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child
2. Information may be provided in writing, or electronically or by other means
3. The data subject may request the information orally (e.g. over the telephone or face to face), as long as the identity of the data subject has been established
4. We must act on a request from a data subject, unless we are unable to establish their identity
5. We must provide information without undue delay and within a maximum of one month from the receipt of the request
6. The response timescale may be extended by up to two further months for complex or a high volume of requests – the data subject must be informed of this within one month of the request, and the reasons for the delay given
7. If a request is made via electronic form, the response should be via electronic means where possible, unless the data subject requests otherwise
8. If it is decided that we will not comply with a request, we must inform the data subject without delay and at the latest within a month, stating the reason(s) and informing the data subject of their right to complain to the supervisory authority
9. Generally, responses to requests will be made free of charge, unless they are *"manifestly unfounded or excessive" (GDPR Article 12)*, in which case we will either charge a reasonable fee or refuse to action the request
10. If there is doubt about a data subject's identity, we may request further information to establish it

Please refer to the exact text of the GDPR if clarification of any of the above is required.

The procedure for responding to requests from data subjects is set out in Figure 1 and expanded on in Table 1. The specifics of each step in the procedure will vary according to the type of request involved – refer to the relevant section of this procedure for more detail.

2.2 Procedure Flowchart

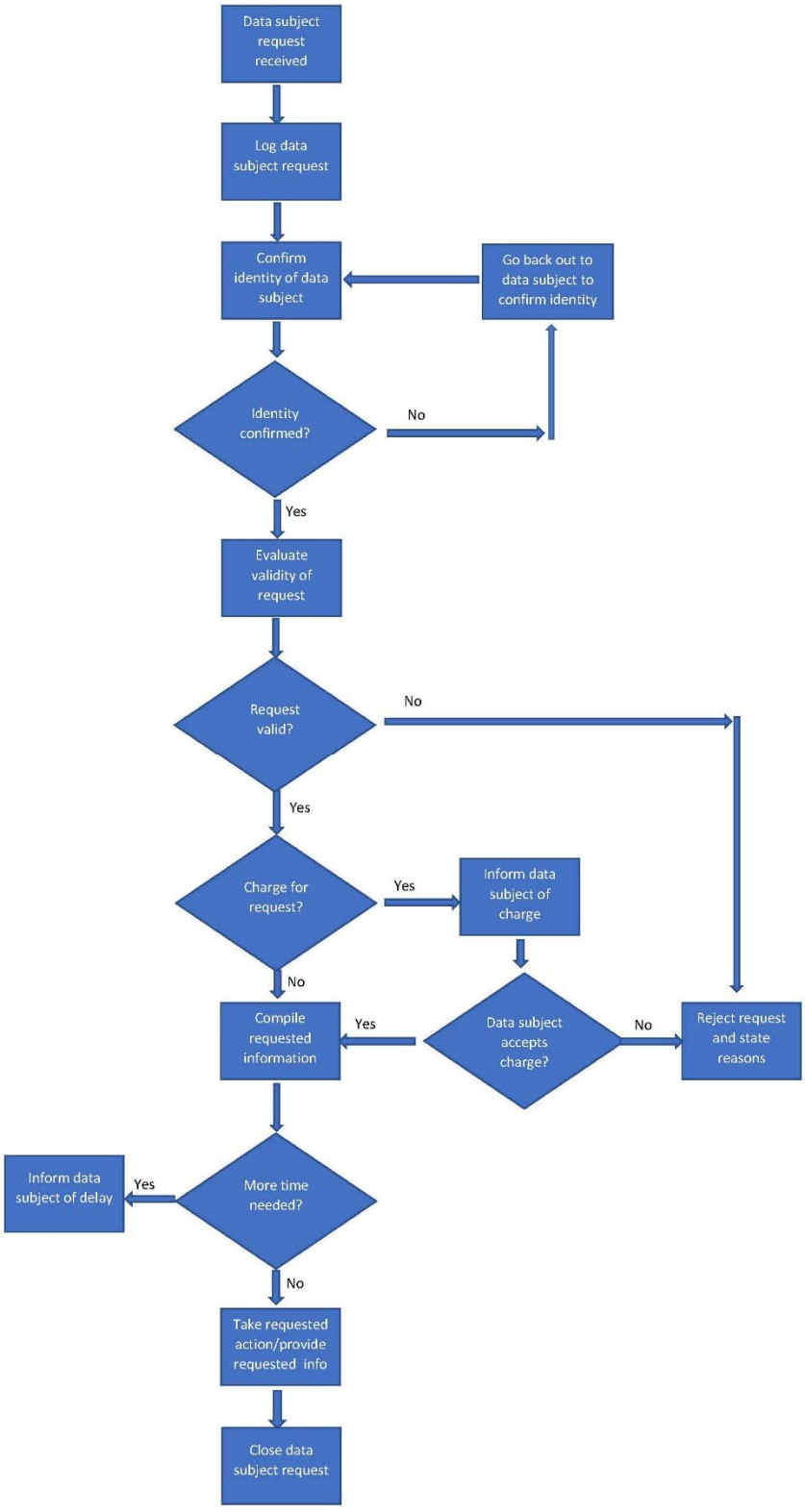

Figure 1 - Data subject request procedure flowchart

2.3 Procedure Steps

The steps depicted in the flowchart in Figure 1 are expanded upon in Table 1 and further under the section addressing each type of request.

Step	Description	Person
Data subject request received	The data subject submits a request via one of a number of methods, including electronically (via email or via our website), by letter or on the telephone. A *Data Subject Request Form* is available for this purpose. Requests may be received by any part of the organisation but should be forwarded to Information Governance, along with the date they were received, as quickly as possible to prevent delays.	Information Governance Team All Staff
Log data subject request	The fact that the request has been received is logged and the date of the request recorded.	Information Governance Team
Confirm identity of data subject	The identity of the data subject is confirmed via an approved method. More information may be requested to confirm identity if required. If the identity of the data subject cannot be confirmed, the request is rejected and the reason for this communicated to the data subject.	Information Governance Team
Evaluate validity of request	The test of whether the request is *"manifestly unfounded or excessive"* is applied. If so, a decision is made whether to reject the request or apply a charge to it. In the case of requests for rectification, erasure, restriction of, or objection to, processing, a decision is also taken about whether the request is reasonable and lawful. If not, the request is rejected and the data subject informed of the decision and their right to complain to the supervisory authority.	Information Governance Team Data Protection Officer
Charge for request	If a charge is applied, the data subject is informed of the charge and has an opportunity to decide whether or not to proceed. If the data subject decides not to proceed, the request is rejected and the reasons communicated.	Information Governance Team Data Protection Officer

Step	Description	Person
Compile requested information	The relevant information is compiled according to the type of request. This may involve planning how the requested action, e.g. erasure or restriction of processing, will be achieved. A maximum of one month is permitted; if the request will take longer than that then a maximum of two further months are allowed and the data subject must be informed of the delay and the reasons for it within one month of the request being submitted.	Information Governance Team
Take requested action/provide requested information	The requested action is carried out (if applicable) and confirmed to the IG Team. The information is provided to the Information Governance Team for review.	Information Asset Owner Individual Staff Member
Provide response / requested information	Confirmation of action taken / the information requested is provided to the data subject electronically, if that is the preferred method, or via other means.	Information Governance Team
Close data subject request	The fact that the request has been responded to is logged in the *Data Subject Request Register*, together with the date of closure.	Information Governance Team

Table 1 - Procedure steps

2.4 The right to withdraw consent

The data subject has the right to withdraw consent where the basis for processing of their personal data is that of consent (i.e. the processing is not based on a different justification allowed by the GDPR such as contractual or legal obligation).

Before excluding the data subject's personal data from processing, it must be confirmed that consent is indeed the basis of the processing. If not, then the request may be rejected on the grounds that the processing does not require the data subject's consent. Otherwise, the request should be allowed.

In many cases, the giving and withdrawal of consent will be available electronically i.e. online, and this procedure will not be required.

Where consent involves a child (defined by the Data Protection Bill as age 13 or under) the giving or withdrawal must be authorised by the holder of parental responsibility over the child.

2.5 The right to be informed

At the point where personal data are collected from the data subject or obtained from another source, there is a requirement to inform the data subject about our use of that data and their rights over it. Compliance with this right is addressed in a separate document, *Privacy Notice Procedure,* which describes the information that must be provided and sets out how and when this must be achieved.

2.6 The right of access

A data subject has the right to ask the University of Exeter whether we process data about them, to have access to that data and in addition the following information:

1. The purposes of the processing
2. The categories of the personal data concerned
3. The recipients, or categories of recipients, of the data, if any, in particular any third countries or international organisations
4. The length of time that the personal data be stored for (or the criteria used to determine that period)
5. The data subject's rights to rectification or erasure of their personal data and restriction of, or objection to, its processing
6. The data subject's right to lodge a complaint with a supervisory authority
7. Information about the source of the data, if not directly from the data subject
8. Whether the personal data will be subject to automated processing, including profiling and, if so, the logic and potential consequences involved
9. Where the data are transferred to a third country or international organisation, information about the safeguards that apply

In most cases, the decision-making process for such requests will be straightforward unless it is judged that the request is manifestly unfounded or excessive. The compilation of the information is likely to require the input of the data owner.

2.7 The right to rectification

Where personal data is inaccurate, the data subject has the right to request that it be corrected and incomplete personal data completed based on information they may provide.

Where necessary, the University of Exeter will take steps to validate the information provided by the data subject to ensure that it is accurate before amending it.

2.8 The right to erasure

Also known as "the right to be forgotten", the data subject has the right to require the University of Exeter to erase personal data about them without undue delay where one of the following applies:

- The personal data are no longer necessary for the purpose for which they were collected
- The data subject withdraws consent and there is no other legal ground for processing
- The data subject objects to the processing of the personal data
- The personal data have been unlawfully processed
- For compliance reasons, i.e. where it needs to be removed to meet the legal obligations of the University of Exeter.
- Where the personal data was relevant to the data subject as a child

Reasonable efforts must be made to ensure erasure where the personal data has been made public.

The University of Exeter will need to make a decision on each case of such requests as to whether the request can or should be declined for one of the following reasons:

- Right of freedom of expression and information
- Compliance with a legal obligation
- Public interest in the area of public health
- To protect archiving purposes in the public interest
- The personal data is relevant to a legal claim

It is likely that such decisions will require the involvement of the University of Exeter Data Protection Officer and in some cases senior management.

2.9 The right to restrict processing

The data subject can exercise the right to a restriction of processing of their personal data in one of the following circumstances:

- Where the data subject contests the accuracy of the data, until we have been able to verify its accuracy
- As an alternative to erasure in the circumstances that the processing is unlawful
- Where the data subject needs the data for legal claims but it is no longer required by us
- Whilst a decision on an objection to processing is pending

The University of Exeter will need to make a decision on each case of such requests as to whether the request should be allowed. It is likely that such decisions will require the involvement of the University of Exeter's Data Protection Officer and in some cases senior management.

Where a restriction of processing is in place, the data may be stored but not processed without the data subject's consent, unless for legal reasons (in which case the data subject must be informed). Other organisations who may process the data on our behalf must also be informed of the restriction.

2.10 The right to data portability

The data subject has the right to request that their personal data be provided to them in a *"structured, commonly-used and machine-readable format" (GDPR Article 20)* and to transfer that data to another party e.g. service provider. This applies to personal data provided by the data subject in a machine readable format for which processing is based on the data subject's consent or on a contract and the processing carried out by automated means.

Where feasible, the data subject can also request that the personal data be transferred directly from our systems to those of another provider.

2.11 The right to object

The data subject has the right to object to processing that is based on the following legal justifications:

- For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- For the purposes of the legitimate interests of the controller

Once an objection has been made, the University of Exeter must justify the grounds on which the processing is based and suspend processing until this is done. Where the personal data is used for direct marketing purposes we have no choice but to no longer process the data.

2.12 Rights in relation to automated decision making and profiling

The data subject has the right to not be the subject of automated decision-making where the decision has a significant effect on them, and can insist on human intervention where appropriate. The data subject also has the right to express their point of view and contest decisions.

There are exceptions to this right, which are if the decision:

- Is necessary for a contract
- Is authorised by law
- Is based on the data subject's explicit consent

In assessing these types of request, a judgement needs to be made about whether the above exceptions apply in the particular case in question.

2.13 Summary of Data Subject Rights by Lawful Basis of Processing

The following table shows which rights of the data subject are relevant to each basis of lawful processing. It should be used as a general guide only, as the specific circumstances may affect the validity of the request.

Right of the data subject	Basis of lawful processing					
	Consent	Contractual	Legal Obligation	Vital interests	Public interest	Legitimate interest
Withdraw consent	Yes	No	No	No	No	No
Be informed	Yes	Yes	Yes	Yes	Yes	Yes
Access	Yes	Yes	Yes	Yes	Yes	Yes
Rectification	Yes	Yes	Yes	Yes	Yes	Yes
Erasure	Yes	No	No	No	No	Yes
Restrict processing	Yes	Yes	Yes	Yes	Yes	Yes
Data portability	Yes	Yes	No	No	No	No
Object	N/A	No	No	No	Yes	Yes
Automated decision making and profiling	N/A	No	No	Yes	Yes	Yes

Table 2 - Applicable rights based on lawful basis of processing

Note

All of the above assume that:

1. the personal data are being lawfully processed
2. the personal data are necessary in relation to the purposes for which they were collected or otherwise processed

If this is not the case, then further investigation must be made regarding the validity of the request.