



The James
Hutton
Institute

James Hutton Group

Data Subject Access Request (SAR) Policy, Guidance and Template

Prepared By: DPO
Date: 30 September 2018

Approved By: DPO
Date: 30 September 2018

Summary of Changes Since Previous Version:

New Policy

Contents

1.0 Introduction and Scope

2.0 Overview: Data Subject Rights

3.0 Subject Access Request – Procedure for responding

4.0 Subject Access Request – Additional Information for Inclusion in Responses

5.0 Exceptions to the Data Subject Rights

Appendix 1

Appendix 2

[Policy Title]

1.0 Overview and Scope

This document applies to the employees, staff, workers and/or other individuals working or undertaking a role under or on behalf of the James Hutton Group which consists of The James Hutton Institute (“Hutton”) including Biomathematics & Statistics Scotland (“BioSS”) and James Hutton Limited (“JHL”). Hutton is a data controller in respect of all personal data it processes and JHL is a data controller in respect of the personal data it processes. When the terms ‘we’, ‘us’ or ‘our’ are used it should be read as referring to the James Hutton Group, unless otherwise specified.

The General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (“the 2018 Act”) provide data subjects with a variety of rights in relation to the personal data held about them by Hutton. A summary of these rights are set out below.

It is important to note that data subjects have the right to appeal any decision made by Hutton in response to any data subject request to the Information Commissioner’s Office (“ICO”). In the event the ICO finds that Hutton has infringed rights of a data subject, Hutton could be exposed to ICO action including a monetary penalty of the higher of 4% of Hutton’s annual global turnover or €20M. Therefore it is important that Hutton treats all individuals fairly and each data subject request is handled in accordance with this policy and legal requirements.

Members of staff etc. should consult Hutton’s Information Governance Officer on SAR@hutton.ac.uk if they receive a data subject right request.

The following definitions are applicable to this policy:

Personal Data: means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category of Data: means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

For the purpose of this policy, when we are referring to ‘personal data’, we are referring to Personal Data and Special Category of Data collectively.

Overview of Rights of Data Subjects

Data Subject Rights include:

- 2.1.1 Right to be informed – data subjects have the right (subject to a few exceptions) to be provided with information on how their personal data will be handled by Hutton. Arts 12 – 14 of GDPR set out the information that must be provided and typically this information is provided by way of a privacy notice. Hutton has taken steps to meet its requirements in this regard by updating its employee privacy notice, PhD privacy notice and website privacy notice and will continue to monitor this issue to ensure the correct information is being given at the appropriate times. Please see Hutton Privacy Notice Policy and Guide if you feel a privacy statement is required.
- 2.1.2 Right of access to their personal data – the purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the legality of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any personal data that Hutton holds about them which includes copies of email correspondence referring to them or opinions expressed about them.
- 2.1.3 Right to Rectification - the right of individuals to require Hutton to rectify inaccuracies in personal data held about them. In some circumstances, if personal data is not complete, an individual can require the controller to complete the data, or to record a supplementary statement.
- 2.1.4 Right to be forgotten (erasure) – Individuals have the right to have their data erased in certain situations such as where the data is no longer required for the purpose for which it was collected, the individual withdraws consent, the individual has objected to processing based on legitimate interests, public task or official authority or the information is being processed unlawfully. There are certain exemptions to this right and there is no absolute obligation on Hutton to erase the relevant data – it is important to identify whether any exemptions apply.
- 2.1.5 Right to Restriction - Individuals can ask Hutton to ‘restrict’ processing of the personal data whilst complaints (for example, about accuracy) are resolved. Individuals can also ask Hutton to restrict processing where the processing is unlawful, Hutton no longer needs the personal data but the individual does not want it erased and/or the individual has objected to the processing and while the objection is being considered, the individual wishes their data restricted.
- 2.1.6 Right to Portability – the data subject has the right to request that personal data concerning them and held by Hutton is provided to the individual (or a third party) in a structured, commonly used and machine-readable form. This right only applies to personal data that is processed by automated means (not paper records) and the processing is based either on consent or contract.

2.1.7 Right to Object – data subjects have the right to object to specific types of processing based on (i) public interest/official authority; or (ii) legitimate interests; or where it involves processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right. If Hutton receives an objection to direct marketing, it must stop processing the personal data for this purpose immediately. Otherwise, Hutton is entitled to consider whether there is legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or whether it needs to process the personal data for the establishment, exercise or defence of legal claims; in both cases Hutton can override the objection.

2.1.8 Rights in relation to automated decision making and profiling – the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. “Profiling” is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. The foregoing right does not apply if: (a) it is necessary to enter into a contract with the data subject and Hutton; (b) it is authorised by applicable law (and such law lays down suitable measures to safeguard the data subjects rights and freedoms and legitimate interest) or (c) is based on the data subject’s explicit consent. However, even if (a) or (c) is relevant, please note that Hutton must put in place suitable measures to safeguard the rights of the data subject including the right to ask for a human to review the decision on behalf of Hutton and to contest the decision. Further, automated decision-taking based on special category of data can only be done with explicit consent.

3. Response Procedure

3.1 General:

- a) Communication:- any communication with the data subject when responding to any request must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Communication should be in writing or by other means if appropriate e.g. electronic means. It can also be provided orally if requested by the data subject, provided that Hutton is satisfied of the identity of the data subject and this is proven by other means. Where the request is by electronic means, the information should be provided electronically where possible, unless otherwise requested by the data subject;
- b) Timing: - any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month of receiving the request. There may be some circumstances where Hutton can take longer than one month to fulfil the request (up to a maximum two further months where the request is complex or high number of requests being dealt with) however these are limited and Hutton should always strive to meet the

one month timeframe wherever possible. If Hutton needs to extend the response deadline, it must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay;

- c) Costs - in most circumstances Hutton will not be able to charge a fee for responding to any data subject request, unless the requests are manifestly unfounded or excessive in particular because of their repetitive character. In this case, Hutton will have to demonstrate how the request is manifestly unfounded or excessive in character and can either charge a reasonable fee taking into account the administrative costs of providing the information or communication, taking the action required or refuse to act on the request.

- 3.2 Step One: - Hutton should acknowledge receipt of a data subject request and confirm that Hutton is looking into the request and will respond within the statutory timeframe. Our letter acknowledgment template can be found at Appendix 1 of this Policy and must be used in response to each data subject request.

If Hutton has concerns over the identity of the natural person making the request, Hutton may request the provision of additional information necessary to confirm the identity of the data subject, which has the effect of 'stopping the clock'. Hutton would not be obliged to respond to the request until it is satisfied of the identity of the person (acting reasonably). Please note it is possible that Hutton may receive requests for a third party on behalf of a data subject e.g. a solicitor or a power of attorney or a friend.

In these cases, Hutton needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If Hutton is of the view that the data subject may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, Hutton may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it. In many respects, this would be the safest option for Hutton in this scenario.

- 3.3 Step Two: - assess whether Hutton requires to extend the deadline to respond to the request and/ or whether it needs additional information before responding and communicate this to the data subject as soon as possible and no later than one month following receipt of the request.
- 3.4 Step Three: - identify relevant personal data. This can take some time to accumulate therefore it is recommended to start the process as soon as possible following Step Two.
- 3.5 Step Four: - identify whether any exemption applies. It is important to remember that there are circumstances where Hutton would not require to comply with the data subject's request as referred to above in the explanation of the rights. There are also further exemptions set out in section 15 of the 2018 Act. Each request should be considered on its own merit and

in relation to the facts and circumstances at the time. Basic information on the exceptions to the above data subject rights can be found at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>. The 2018 Act is a complex piece of legislation and provision of detailed explanation of exemptions is out side the scope of this policy. The Responsible Person should consider the detail of exemptions carefully. Please also see section 5 of this policy for guidance.

3.6 Step Five:

- a) (Scenario A): - if, having considered the data subject request, Hutton decides not to comply in full because an exemption applies, an explanation must be provided to the individual within the deadline, informing them of their right to complain to the ICO and their right to seek a judicial remedy;
- b) (Scenario B): - if, having considered the data subject request, Hutton decides that an exemption does not apply at all, Hutton must comply with the request and confirm compliance/disclose the relevant information within the statutory timeframe as above;
- c) (Scenario C): - if, having considered the data subject request, Hutton decides that an exemption applies in part, it should communicate to the data subject within the statutory timeframe its response and where the request is a data subject access request provide the necessary information with the non-disclosable information redacted where appropriate. The data subject should be informed of their right to complain to the ICO and their right to seek a judicial remedy.

3.7 Step Six: Tracking Requests and Responses: - data subject requests must be tracked and recorded by Hutton for accountability purposes.

4. Subject Access Request Procedure

4.1 All Subject Access Requests received by Hutton will be processed by the Information Governance Officer (IGO). Any requests received by Hutton staff should be e-mailed to the IGO (SAR@hutton.ac.uk) without delay in order that a response can be issued within the statutory deadline of one month.

The right to access their personal data is one of the most likely forms of subject requests Hutton will receive. The above information applies equally to data subject access requests. However it should be noted that when responding to data subject access requests, data subjects are also entitled (unless an exemption applies) to be informed of the following:

- a) Confirmation that personal data about them is being processed.
- b) A copy of that personal data.
- c) Details of the purpose of the processing.
- d) Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information.

- e) Any recipients or categories of recipients the personal information has been shared with, particularly if these are situated or domiciled outside the EU.
- f) What safeguards are in place for transfers out with the EU.
- g) The period the personal information will be stored for or what the criteria are for determining the period of storage.
- h) The existence of the right to request from the data controller the correction or deletion of personal data or to restrict or object to the processing of personal data concerning them.
- i) The right to lodge a complaint with the Information Commissioner's Office.
- j) The source of the personal data if it has not been collected directly from the data subject.
- k) Details of any automated decision-making, including profiling, and meaningful information about the logic involved and the envisaged consequences of such processing for the data subject.

4.2 As above, each data subject access request should be reviewed on its own merit and each time, Hutton should consider whether an exemption to disclosure applies. Section 15 of the 2018 Act sets out when organisations may refuse in whole or in part a data subject access request and information can be found here: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/> As a general rule however, personal data relating to other individuals should not be disclosed (unless their permission has been obtained to release it or it is reasonable to comply without consent), therefore if this is within the requested information, Hutton should generally redact such information.

5. Exceptions to the Data Subject Rights

5.1 Section 15 of the 2018 Act sets out the exceptions to the rights vest in data subjects. The applicability of these should be reviewed on a case by case basis and it can be a complex area of law. Where appropriate, legal advice ought to be obtained. In summary, the main exceptions likely to be applicable include for reasons related to:-

- a) Protecting the personal data of third parties;
- b) Legal professional privilege;
- c) Prevention or detection of crime;
- d) Apprehension or prosecution of offenders;
- e) Assessment or collection of tax or duty;
- f) Immigration;
- g) Information required to be disclosed by law or in relation to legal proceedings.

Appendix 1: Acknowledgment of Data Subject Request Letter Template

[DATA SUBJECT NAME/REQUESTER NAME]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE/CITY]

[COUNTRY]

[DATE]

Dear [DATA SUBJECT NAME/REQUESTER NAME]:

Reference: [DATA SUBJECT REQUEST TYPE/REFERENCE NUMBER]

We write to acknowledge receipt of your request dated [DATE] made under Article [NUMBER] of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). We received your request on [DATE].

The GDPR requires us to respond to requests within one month of receipt. We expect to provide a response by [DATE]. However, in certain circumstances, the GDPR or other applicable law allows us to extend that deadline by two months depending on the complexity of your request. We will advise you within one month if we need to extend the response deadline.

Our initial response letter may also advise you that:

We require more information to verify [your identity/your legal authority to make the request on another individual's behalf].

We need more information to respond to the request.

We require you to pay a fee before we respond to the request.

If we cannot honour the request, we will inform you of the reasons why, subject to any legal or regulatory restrictions by [DATE].

If you have any questions on the status of the request, please contact [NAME AND TITLE] at [TELEPHONE NUMBER] or [EMAIL ADDRESS]. [To check the status of the request, you may also use [our secure portal/[SUBMISSION MECHANISM]], after authenticating your identity with your [username and password/[OTHER AUTHENTICATION MECHANISM]].]

Sincerely,

[SENDER NAME] For and on behalf of [James Hutton Institute/James Hutton Limited]

Appendix 2: Data Subject Access Request Form

James Hutton [Institute/Limited]

Data Subject Access Request Form

Article 15 of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) grants you the right to access your personal data held by [James Hutton Institute] or [James Hutton Limited] or [BioSS], including the right to obtain confirmation that we process your personal data, receive certain information about the processing of your personal data, and obtain a copy of the personal data we process. We request that you submit this electronically via email to our Information Governance Officer at SAR@hutton.ac.uk. Please note use of this form is not mandatory and you may submit your request in other formats e.g. plain email if that is preferable.

We expect to respond to your request within one month of receipt of a fully completed form and proof of identity.

I. Requester Name (Data Subject) and Contact Information

Please provide the data subject's information in the space provided below. If you are making this request on the data subject's behalf, you should provide your name and contact information in Section III.

We will only use the information you provide on this form to identify you and the personal data you are requesting access to, and to respond to your request.

First and last name:	
Any other names that you have been known by (including nicknames):	
Home address:	
Date of birth:	
Telephone number:	
Email address:	
If you are a current or former employee of Hutton please provide your employee identification number and your approximate dates of employment:	

<p>Please provide other unique identifiers or related information to help us locate your personal data (for example, government identification number or customer account number):</p>	
---	--

[II. Proof of Data Subject's Identity

We require proof of your identity before we can respond to your access request. To help us establish your identity, you must provide identification that clearly shows your name, date of birth, and current address. We accept a photocopy or a scanned image of one of the following as proof of identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. If you have changed your name, please provide the relevant documents evidencing the change.

If you do not have any of these forms of identification available, please contact Hutton for advice on other acceptable forms of identification.

We may request additional information from you to help confirm your identity and your right to access, and to provide you with the personal data we hold about you.

[III. Requests Made on a Data Subject's Behalf

Please complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

First and last name:	
Home address:	
Date of birth:	
Telephone number:	
Email address:	

We accept a photocopy or a scanned image of one of the following as proof of your identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. If you do not have any of these forms of identification available, please Hutton for advice on other acceptable forms of identification. We may request additional information from you to help confirm your identity if necessary.

We also require proof of the data subject's identity before we can respond to the request. To help us establish the data subject's identity, you must provide identification that clearly shows the data subject's name, date of birth, and current address. We accept a photocopy or a scanned image of one of the following as proof of identity: passport or photo identification such as a driver's license, national identification number card, or birth or adoption certificate. If the data subject has changed their name, please provide the relevant documents evidencing the change.

We accept a copy of the following as proof of your legal authority to act on the data subject's behalf: a written consent signed by the data subject, a certified copy of a Power of Attorney, or evidence of parental responsibility.

We may request additional information from you to help confirm the data subject's identity. We reserve the right to refuse to act on your request if we are unable to verify your legal authority to act on the data subject's behalf.

IV. Information Requested

To help us process your request quickly and efficiently, please provide as much detail as possible about the personal data you are requesting access to. Please include time frames, dates, names, types of documents, file numbers, or any other information to help us locate your personal data.

For example, you may specify that you are seeking:

Employment records or personnel records.

Personal data held by a specific department of Hutton

Medical records.

E-mail or other electronic communications (specify the approximate dates and times).

Billing information.

Photographs.

Video footage.

User activity logs.

Transaction histories

Correspondence between [NAME] and [NAME] between [DATE] and [DATE].

We will contact you for additional information if the scope of your request is unclear or does not provide sufficient information for us to conduct a search (for example, if you request "all information about me"). We will begin processing your access request as soon as we have verified your identity and have all of the information we need to locate your personal data.

Description of Data Requested

If the information you request reveals personal data about a third party, we will either seek that individual's consent before responding to your request, disclose it, or we will redact third parties' personal data before responding. If we are unable to provide you with access to your personal data because disclosure would violate the rights and freedoms of third parties, we will notify you of this decision.

Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

V. Signature and Acknowledgment

I, _____, confirm that the information provided on this form is correct and that I am the person whose name appears on this form. I understand that: (1) Hutton must confirm proof of identity and may need to contact me again for further information; (2) my request will not be valid until Hutton receives all of the required information to process the request; and (3) I am entitled to one free copy of the personal data I have requested, and acknowledge that for any further copies I request, Hutton may charge a reasonable fee based on administrative costs.

If you would like to receive a copy of the personal data you are requesting access to, please indicate below whether you would like a hard copy or an electronic copy:

Hard copy.

Electronic copy.

Signature

Date

[VI. Authorized Person Signature

I, _____, confirm that I am authorised to act on behalf of the data subject. I understand that Hutton must confirm my identity and my legal authority to act on the data subject's behalf, and may need to request additional verifying information.

Signature

Date]

Version Control

Title	Subject Access Request Policy, Guide and Template
Author/Creator	Data Protection Officer
Owner	Data Protection Officer
Date Published/Approved	30 September 2018
Version	FINAL.V1.Sept2018
Date of Next Review	August 2019
Audience	All Hutton Staff and Stakeholders
Related Documents	GDPR Policy
Subject/Description	Policy provides guidance and processes relating to the administration of Subject Access Requests.
Group	FCS
Department	Research Support