Exercising Data Subject Rights Procedure

1 Introduction

GDPR gives data subjects a number of rights to enable to understand how their data is being processed and to ensure it is managed appropriately by organisations, or where appropriate, that processing cease. Many of these rights are qualified, and if the University of Nottingham can demonstrate the legitimacy of processing, it may be able to refuse to comply with a request from a data subject.

2 Aim

This procedure explains the rights given to a data subject and sets out the mechanisms by which data subjects can exercise them, and how UoN will respond.

3 Responsibilities

All staff processing personal data are responsible for ensuring that data subjects are able to exercise their rights on demand. Data subjects are to be encouraged to contact the Information Compliance team in the first instance, who will then liaise with Data Asset Owners or Data Stewards as appropriate. However, data subjects are entitled to contact anyone in the organisation to make a request to exercise their rights. Staff receiving a request should make the Information Compliance team aware in the first instance.

4 Communication

This procedure will be published on the University's internal website. Rights are identified to data subjects as part of the University's privacy notices on the public website. Line managers are responsible for bringing this policy to the attention of members of staff in their area, including new staff.

5 Revision

This procedure will be revised regularly, and formally approved by the Information Management and Security Steering Committee on a regular basis.

Approved: 21 May 2018

Next revision due: July 2019

6 Contact

Fraser Marshall
Governance and Quality Manager
fraser.marshall@nottingham.ac.uk

Procedure for exercising data subjects' rights
1 Right to be informed
This right concerns UoN's obligation to provide 'fair processing information' which is concise, transparent, intelligible and easily accessible, free of charge, and which is written in clear and plain language, particularly if aimed at children. Keeping a record of how we use personal data demonstrates compliance with the need for accountability and transparency. The university will ensure a data subject has sufficient information to ensure that they're happy about how and why the University is handling their personal data, and that they know how to enforce their rights. The University provides information in the form of privacy notices. The Privacy Notice Procedure can be found on the University's website.
2 Right of access
Individuals have the right to access their personal data and supplementary information. They are entitled to be aware of what data UoN holds and be able to verify the lawfulness of the processing of that data. Individuals wishing to make a request for their own data should be directed to https://www.nottingham.ac.uk/governance/records-and-information-management/data-protection/data-protection.aspx The University will use the Responding to Data Subject Access Requests (SARs) procedure to process requests.
3 Right to data portability
Individuals can request a copy of their data for their own purposes. It allows individuals to obtain and reuse their personal data across different services and allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This right applies where data is held electronically in a structured form, such as in a database, and our lawful basis for processing this information is consent or for the performance of a contract. To receive their information in a portable form, data subjects should send an email with their request to data-protection@nottingham.ac.uk. The Information Compliance team will liaise with the Data Asset Owner or Data Steward[1] of the requested data. The Data Asset Owner/Steward is required to provide the information to a data subject within one calendar month in a structured, commonly-used and machine readable format, or provide access to an automated tool to allow the individual to extract the requested data themselves, unless to do so would cause a risk to the rights and freedoms of others. We must send the data directly to another controller if requested. Where a request is not deemed appropriate, the data subject must be informed of the reason, their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

[1] as defined in the Data Handling Policy

4 Right of rectification

Where data is incorrect or incomplete, individuals are entitled to have it corrected. Corrections must be passed to any parties with whom the data has been shared.

Requests for correction to personal data can be made verbally. Requesters should be encouraged to make a request by sending an email outlining the corrections required to data-protection@nottingham.ac.uk.

The Information Compliance team will liaise with the Data Asset Owner or Data Steward of the requested data.

Where a request for rectification is deemed appropriate, the Data Asset Owner/Steward is required to amend the information of a data subject without delay, and no later than one month after receiving the request, unless the DPO has given permission to extend the deadline by up to another month. The Data Asset Owner/Steward must communicate that this amendment has been made to the data subject. Where necessary to retain the integrity of the University's records, a narrative may be recorded to retain the incorrect data and any consequences that have arisen through its use.

Where a request is not deemed appropriate, the data subject must be informed of the reason, their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

5 Right to erasure

AKA 'the right to be forgotten'. Individuals can request the deletion or removal of personal data where there is no compelling business reason for its continued processing. The circumstances in which data can be deleted are as follows:

- the personal data is no longer necessary for the purpose which UoN originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child

We do not have to erase data if we are processing it

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

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

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

We can refuse to comply with a request for erasure if it is manifestly unfounded or excessive (especially if the request is repetitive), or request a "reasonable fee" to deal with the request. Where a fee is requested, the data subject must also be informed of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

Requests for erasure of personal data can be made verbally. Requesters should be encouraged to make a request by sending an email the data they require deleting to data-protection@nottingham.ac.uk.

The Information Compliance team will liaise with the Data Asset Owner or Data Steward of the requested data to determine whether it is legitimate to erase the data.

Where a request for erasure is deemed appropriate, the Data Asset Owner/Steward is required to permanently erase the information of a data subject without delay, and no later than one month after receiving the request, unless the University has extended – check other places including page 5 the deadline by up to another month. The Data Asset Owner/Steward must communicate that this amendment has been made to the data subject.

Where a request is not deemed appropriate, the data subject must be informed of the reason, their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

6 Right to restrict processing

If individuals think there is a problem with the accuracy of the data UoN holds about them, or we're using data about them unlawfully, they can request that any current processing is suspended until a resolution is agreed.

Requests for restriction of processing can be made verbally. Requesters should be encouraged to make a request by sending an email the data they require deleting to data-protection@nottingham.ac.uk.

The Information Compliance team will liaise with the Data Asset Owner or Data Steward of the requested data to determine whether it is legitimate to erase the data.

Where a request for erasure is deemed appropriate, the Data Asset Owner/Steward is required to permanently erase the information of a data subject without delay, and no later than one month after receiving the request, unless the DPO has given permission to extend the deadline by up to another month. The Data Asset Owner/Steward must communicate that this amendment has been made to the data subject.

7 Right to object

Data subjects have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Processing based on legitimate interests/ the performance of a task in the public interest/exercise of official authority (including profiling)
Unless UoN can demonstrate a compelling case why our use of data is justified, which overrides the interests, rights and freedoms of the individual, or the processing is for the establishment, exercise or defence of legal claims, we have to stop using a data subject's personal data upon receipt of an objection.

Direct marketing (including profiling)
For direct marketing, there will be an opt-out provided with each marketing message communicated. Where a data subject exercises their right to opt out of direct marketing, the University must as soon as possible cease to send direct marketing material to the individual.

Processing for purposes of scientific/historical research and statistics
Individuals must have 'grounds relating to their particular situation' in order to exercise their right to object to processing for research purposes. Research by universities has been determined to be in the public interest, and this means that we are not required to comply with an objection to processing if the objection would cause disproportionate cost or disruption.

Objections must be made in writing, preferably by email to data-protection@nottingham.ac.uk.

The Information Compliance team will liaise with the Data Asset Owner or Data Steward of the requested data to determine whether it is required to comply with the objection.

Where an objection is deemed appropriate, the Data Asset Owner/Steward is required to cease the processing that has given rise to the objection without delay.

8 Rights related to automated decisions making including profiling

UoN may use a computer program to make decisions about a data subject without human involvement – for example, everyone that is on a particular course gets sent a particular letter – or to profile individuals according to an evaluation of certain characteristics. Data subjects have a right to ask for someone to intervene on their behalf or to check a decision if the automated decision making/profiling produces legal effects concerning the data subject or similarly significantly affects them.

This right cannot be invoked if the processing:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

Requests for a review of automated decision making or profiling must be made in writing, preferably by email to data-protection@nottingham.ac.uk.

The Information Compliance team will liaise with the Data Asset Owner or Data Steward of the requested data to determine whether it is required to comply with the objection.

Where an objection is deemed appropriate, the Data Asset Owner/Steward is required to appoint appropriate individual(s) with the necessary technical and business process skills to review the decision or profiling without delay and in any case within a month.

9 In all situations where a data subject seeks to exercise a right in respect of their personal data:

- UoN is entitled to verify the identity of the requester using the same means as set out in the Subject Access Request Procedure
- where a requester wishes to make a request verbally, the person receiving the request must contact the requester in writing and set out their understanding of the erasure required and provide an opportunity for the requester to feedback
- the Data Asset Owner/Steward will ensure that where a data subject's data has been transferred to a third party recipient, that the right has been invoked by the data subject and the result of that request at UoN is communicated to the third party recipient
- where possible, UoN will seek to provide data subjects with the means to view and amend their data via self-service mechanisms such as online portals
- UoN's response to the request to exercise a right must be communicated by Information Compliance team to the data subject and logged

DOCUMENT HISTORY

Date and event	Change Detail
21 May 2018	Procedure approved by IMSSC

RELATED POLICIES AND GUIDANCE

Data Subjects' Rights – a guide

Data Subject Access Request Procedure

Data Subject Access Request Form

Data Protection Policy