



Code: QA
Title: Data Subject Rights Request Procedure
Approval: Approved by ICT Security Committee
Date: 26 March 2019

1. Purpose:

The purpose of this procedure is to ensure that the University complies with the Data Subject rights provisions of the Data Protection Acts 1988-2018 and to enable individuals to submit Data Subject requests where required. “**Data Subjects**” are identified or identifiable natural person(s). A Data Subject has rights under Data Protection Law **as follows:**

- A. Right of access - A Data Subject has the right to request copies of personal data held on her/him. Access requests are governed by Sections 4 and 91 of the Data Protection Act 2018. A copy of both Sections is available at Schedule 1.
- B. Right to rectification - The right to require a Controller to rectify inaccuracies in Personal Data or Special Categories of Personal Data held about them.
- C. Right to erasure (‘right to be forgotten’) Data Subjects have the right to have their data erased in certain situations, such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent, or the information is being processed unlawfully. There is an exemption to this right for scientific, historical or statistical research purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Data Subjects can ask the controller to ‘restrict’ processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.
- D. Right to restriction of processing.
- E. Right to data portability - the Data Subject has the right to request their personal data in a structured, commonly used and machine-readable form so it can be sent to another Controller. This only applies to Personal Data or Special Categories of Personal Data that is processed by automated means (not paper records).
- F. Right to object - Data Subjects have the right to object to specific types of processing such as automated decision making and profiling.

2. Access Requests

2.A Member of the public or student making an access request:

If you wish to make an access request, it must be in writing. Your letter for an access request should be addressed to:

The Data Protection Officer, NUI Galway, Room A129, The Quadrangle, NUI Galway, University Road, Galway; **or by email to:** dataprotection@nuigalway.ie

A data access request should read as follows:

"Dear ... I wish to make an access request under the Data Protection Acts 1988 to 2018....."

To help us to respond to your request, please be as specific as possible about the information you wish to access. Please include any additional details that would help to locate your information - for example, a staff or student number, names of departments/offices that you were associated with, etc.

If you wish a third party to submit a data access request on your behalf (e.g. a family member or solicitor), you must provide written authorisation to allow the University to disclose your personal data to that third party.

2.B Employee/ HR Access Request:

In recognition of the principles of Section 4 Irish Data Protection Act 2018, employees or prospective employees can contact HR directly for a copy of their recruitment process records or HR file.

3. Other Data Protection Right Requests:

If you wish to exercise the right to rectification, right to erasure ('right to be forgotten'), the right to restriction of processing, the right to notification obligation regarding rectification or erasure of personal data or restriction of processing, the right to data portability or the right to object it must be made in writing and it will be considered by the Data Protection Office and the applicable Unit Heads. The written request can be sent to:

The Data Protection Officer, NUI Galway, Room A129, The Quadrangle, NUI Galway, University Road, Galway; **or by email to:** dataprotection@nuigalway.ie

4. Identification:

In order to ensure that personal data is not disclosed to the wrong person, you may be required to provide proof of identity before any personal data is released to you. Acceptable forms of identification include: copy of passport or driving licence; staff/student ID card; copy of bank statement; copy of utility bill. Copies are acceptable in most cases; however we reserve the right to ask to see original documents where necessary. If you are required to provide copies of such documents to the University, they will be securely destroyed once we have verified your identity.

5. Timeline:

A decision on your access requests will be made within 30 days of receipt of your request unless extended in accordance with the provisions of the Data Protection Act 2018.

6. Right to complain to Data Protection Commissioner:

If you are unhappy with the outcome of your request, you may make a complaint to the Data Protection Commissioner (Canal House, Station Road, Portarlinton, Co. Laois), who will investigate the matter for you. Please see: www.dataprotection.ie

7. Further details on your rights:

Further details on your rights under the Data Protection Acts are available on the Data Protection Commissioner's website www.dataprotection.ie and on the NUI Galway Data Protection website: <https://www.nuigalway.ie/data-protection/>

8.0 Responsibilities

The following roles and responsibilities apply in relation to this Procedure:

Name/Title	Roles and Responsibility
ICT Security Committee	Procedure approver.
University Management Team (UMT)	Each member of UMT is responsible for ensuring compliance with the Data Protection Acts and this Procedure in their respective areas of responsibility.
Internal Audit	Monitoring and reporting compliance with the Procedure
Secretary	Procedure Owner. Ensuring that appropriate policies and procedures are in place to support this Procedure. Liaising with the UMT as appropriate.
Data Protection Officer	Act as a contact point and support for and liaising with the Data Subject Requests and liaising with Unit Heads to process requests. Ensuring that this Procedure is reviewed and approved by the ICT Security Committee as appropriate. Organize targeted Procedure training and briefing sessions for University staff as required.
Heads of School/Unit	Ensuring compliance with this Procedure in their respective areas of responsibility. Prompt processing of Data Subject rights requests noting the 30-day time limit. Notification of Breaches to affected Data Subjects if required. Ensuring Personal Data sharing is conducted in accordance with University guidance.
All Staff or Students or Members engaged in dealing with personal or Special Categories of Personal Data	Acquaint themselves with, and abide by, the rules of this Procedure and related policies and procedures. Understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data. Where directed by Unit Head or Data Protection Officer prompt processing of Data Subject rights requests noting the 30-day time limit. Must complete relevant training and awareness activities provided by the University to support compliance with this Policy. Should take all necessary steps to ensure that no breaches of information security result from their actions. Use a minimum of personal data and only hold it for as long as is strictly necessary.

9.0 Related Documents

QA400 Data Protection Policy
 QA402 Data Classification Policy
 QA401 Data Handling Policy
 QA442 Record Retention Policy

Data Breach Procedure
Records of Processing Procedure

10.0 Further Information

If you have any queries in relation to this policy, please contact:

The Data Protection Officer
NUI Galway, Room A129
The Quadrangle
NUI Galway
University Road
Galway
Email: dataprotection@nuigalway.ie
Tel: (091) 492150

11.0 Disclaimer

The University reserves the right to amend or revoke this Procedure at any time without notice and in any manner in which the University sees fit at the absolute discretion of the University or the President of the University.

Schedule 1

Section 4 - Obligation not to require data subject to exercise right of access under Data Protection Regulation and Directive in certain circumstances

4. (1) A person shall not, in connection with—
- (a) the recruitment of an individual as an employee,
 - (b) the continued employment of the individual, or
 - (c) a contract for the provision of services to the person by an individual,
- require that individual to—
- (i) make a request under Article 15 or under *section 91*, or
 - (ii) supply the person with data relating to that individual obtained as a result of such a request.
- (2) A person who contravenes *subsection (1)* shall be guilty of an offence and shall be liable—
- (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
 - (b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

Section 91 of Data Protection Act 2018 - Right of access

An individual who believes that personal data relating to him or her have been or are being processed by or on behalf of a controller, if he or she so requests the controller by notice in writing shall—

- (a) be informed by the controller whether personal data relating to him or her have been or are being processed by or on behalf of the controller, and
 - (b) where such data have been or are being so processed, be provided by the controller with the following information:
 - (i) a description of—
 - (I) the purpose of, and the legal basis for, the processing,
 - (II) the categories of personal data concerned,
 - (III) the recipients or categories of recipients to whom the personal data concerned have been disclosed, and
 - (IV) the period for which the personal data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;
 - (ii) information detailing the right of the data subject to request from the controller the rectification or erasure of the personal data concerned;
 - (iii) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission;
 - (iv) a communication of the personal data concerned;
 - (v) any available information as to the origin of the personal data concerned, unless the communication of that information is contrary to the public interest.
- (2) A controller shall respond to a request made under *subsection (1)* and provide the information specified in *paragraph (b)* thereof to the data subject as soon as may be and, subject to *subsections (4) and (5)*, in any event not later than one month after the date on which the request is made.
- (3) When making a request under *subsection (1)*, the individual making the request shall provide the controller with such information as the controller may reasonably require

to satisfy itself of the identity of the individual and to locate any relevant personal data or information.

- (4) Where a controller has reasonable doubts as to the identity of an individual making a request under *subsection (1)* or reasonably requires additional information to locate any relevant personal data, it may request such additional information from the data subject as may be necessary to confirm his or her identity or to enable it to locate such personal data or information, as the case may be, and the period of time from the making of such a request for additional information until the request is complied with shall not be reckonable for the purposes of *subsection (2)*.
- (5) Where, taking into account the complexity of a request made under *subsection (1)* and the number of such requests received by the controller, the controller is of the opinion that it requires additional time to consider the request, it may, once only and within one month from the date of the receipt of the request, extend the time period referred to in *subsection (2)* by such further period not exceeding 2 months as it may specify by notice in writing to the individual making the request.
- (6) A notice in writing referred to in *subsection (5)* shall include the reason for which the controller is of the opinion that it requires additional time to consider the request made under *subsection (1)*.
- (7) Where information that a controller would otherwise be required to provide to a data subject pursuant to *subsection (1)* includes personal data relating to another individual that would reveal, or would be capable of revealing, the identity of the individual, the controller—
 - (a) shall not, subject to *subsection (8)*, provide the data subject with the information that constitutes such personal data relating to the other individual, and
 - (b) shall provide the data subject with a summary of the personal data concerned that—
 - (i) in so far as is possible, permits the data subject to exercise his or her rights under this Part, and
 - (ii) does not reveal, or is not capable of revealing, the identity of the other individual.
- (8) *Subsection (7)* shall not apply where the individual to whom the personal data that would reveal, or would be capable of revealing, his or her identity, relate consents to the provision of the information concerned to the data subject making a request pursuant to *subsection (1)*.
- (9) *Subsection (1)* shall not apply—
 - (a) in respect of personal data relating to the data subject that consists of an expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential, or
 - (b) to information specified in *paragraph (b)(i)(III)* of that subsection in so far as a recipient referred to therein is a public authority which may receive data in the context of a particular inquiry in accordance with the law of the State.
- (10) Information provided pursuant to a request under *subsection (1)* may take account of any amendment of the personal data concerned made since the receipt of the request by the controller (being an amendment that would have been made irrespective of the receipt of the request) but not of any other amendment.
- (11) The obligations imposed by *subparagraphs (iv) and (v) of subsection (1)(b)* shall be complied with by supplying the data subject with a copy of the information concerned in permanent form unless—
 - (a) the supply of such a copy is not possible or would involve disproportionate effort, or
 - (b) the data subject agrees otherwise.

- (12) Where a controller has previously complied with a request under *subsection (1)*, the controller is not obliged to comply with a subsequent identical or similar request under that subsection by the same individual unless, in the opinion of the controller, a reasonable interval has elapsed between compliance with the previous request and the making of the current request.
- (13) In determining for the purposes of *subsection (12)* whether the reasonable interval specified in that subsection has elapsed, regard shall be had to the nature of the personal data, the purpose for which the personal data are processed and the frequency with which the personal data are altered.
- (14) Where a controller, pursuant to *subsection (12)* refuses to act upon a request under *subsection (1)*, it shall, as soon as practicable, so notify the data subject in writing.